Manual de Auditoría Forense especializado en

Criptoactivos, Moneda Digital y Blockchain

ASOCIACIÓN INTERAMERICANA DE CONTABILIDAD

PRIMERA EDICIÓN



Asociación Interamericana de Contabilidad - AIC

Comisión Técnica Interamericana de Peritaje Contable y Auditoría Forense.



Septiembre 2026

Manual de Auditoría Forense especializado en Criptoactivos, Moneda Digital y Blockchain

Asociación Interamericana de Contabilidad - AIC

Comisión Técnica Interamericana de Peritaje Contable
y Auditoría Forense.

Septiembre 2026

MANUAL DE AUDITORÍA FORENSE
ESPECIALIZADO EN CRIPTOACTIVOS, MONEDA DIGITAL Y BLOCKCHAIN

Primera edición agosto 2026. Edición Electrónica.
©2026 por AIC

Equipo de Trabajo y Coautores

MIEMBRO	PAÍS	CARGO
Richard Gómez Jiménez	Rep. Dom.	Presidente comisión técnica
Andrés A. Hernández Cortes	El Salvador	Vicepresidente comisión técnica
María Noel Ramos Pírez	Uruguay	Secretaria comisión técnica
Ramón Vicente Nicastro		Asesor comisión
Alvin Alberto Ibarra Soto		Asesor comisión
Juan Carlos Rivera Gómez	Colombia	Miembro
Abraham Siliezar Montes	El Salvador	Miembro
Olga Jazmin Carrillo Rey	Colombia	Miembro
Marlene R. Almanza Céspedes	Bolivia	Miembro
Luis Rafael Valdez Tejada		Miembro
Emmanuel R. Giménez Insfran	Paraguay	Miembro
Rafael Eduardo Paredes	Perú	Miembro
Eladio Simón Peña García	Rep. Dom.	Miembro
Mariana M. Arcentales Torres	Ecuador	Miembro.
Marco Antonio Martínez Godoy	Venezuela	Miembro
Favio Oviedo García Zelaya	Honduras	Miembro
Enoc José Morales Pestana	Colombia	Miembro
María del Carmen Velasquez A.	Ecuador	Miembro
Nancy Elizabeth López Verón	Paraguay	Miembro
Cesar Alexis Benites Ocampo	Perú	Miembro
Paul David Prieto Amarilla	Paraguay	Miembro
Alexis Antonio Olivo Jiménez	Rep. Dom.	Miembro
Anselma R. Villalba Cristaldo	Paraguay	Miembro
José Luis Carvajal Cevallos	Ecuador	Miembro
Marcos A. Rodríguez Pereira	Paraguay	Miembro
Jeanni Mirshi Miranda Prado	Bolivia	Miembro

DISEÑO Y DIAGRAMACIÓN
Grupo Nous

ISBN: 978-9945-9482-2-6

Santo Domingo, República Dominicana

Todos los derechos reservados. Cualquier forma de reproducción, distribución, comunicación pública o transformación de esta obra solo se puede realizar con la autorización por escrito de sus titulares. La infracción de estos derechos puede constituir un delito contra la propiedad intelectual.

Contenido

Mensaje del *Presidente de la Asociación Interamericana de Contabilidad (AIC)* 7

Mensajes del *Vicepresidente Asuntos Técnicos de la Asociación Interamericana de Contabilidad - AIC* 11

Mensaje del presidente de la Comisión Técnica Interamericana de Peritaje Contable y Auditoría Forense **15**

Palabras del Presidente de la Subcomisión a cargo del Manual de Auditoría Forence Especializado *en Criptoactivos, Moneda Digital y Blockchai, AIC* 17

Palabras Asesor Técnico de la Subcomisión a cargo del Manual de Auditoría Forence Especializado *en Criptoactivos, Moneda Digital y Blockchai, AIC* 21

PARTE I **29**

Fundamentos Generales de los Criptoactivos y la Tecnología Blockchain ***29***

1|1| ***Introducción a los criptoactivos y activos virtuales*** ***31***

2|2| ***Fundamentos Tecnológicos de Blockchain*** ***45***

3|3| ***Ecosistema financiero digital y nuevos modelos de negocio*** ***59***

PARTE II **75**

Marco Normativo, Contable y Regulatorio **75**

4|4|***Normatividad Internacional Aplicable*** ***77***

5|5|***Tratamiento contable y tributario de criptoactivos*** ***111***

6|6|***Riesgos Jurídicos y Delitos Asociados*** ***241***

PARTE III. **257**

Auditoría Forense Aplicada A Criptoactivos **257**

7|7|***Fundamentos de Auditoría Forense en Blockchain*** ***259***

8|8|***Metodologías de auditoría forense en blockchain*** ***267***

9|9|***Procedimientos de Investigación Financiera Digital*** ***275***

PARTE IV **291**

Herramientas, Analítica y Tecnología Forense **291**

Mensaje del *Presidente de la Asociación Interamericana de Contabilidad (AIC)*

La transformación digital está redefiniendo profundamente la manera en que se generan, transfieren, administran y resguardan los recursos económicos y financieros. La expansión de los criptoactivos, las monedas digitales y la tecnología blockchain plantea nuevas oportunidades para el desarrollo de los mercados, al tiempo que introduce desafíos técnicos, contables, jurídicos y regulatorios que exigen una respuesta profesional cada vez más especializadas.

En este contexto, la Asociación Interamericana de Contabilidad (AIC), fiel a su compromiso con el fortalecimiento de la profesión contable en las Américas, presenta con especial satisfacción esta primera edición del "Manual de Auditoría Forense Especializado en Criptoactivos, Moneda Digital y Blockchain", una obra que representa una contribución significativa al desarrollo del conocimiento técnico, la actualización profesional y la cooperación interamericanas.

La responsabilidad de nuestra profesión trasciende el registro y la presentación de la información financiera. Los contadores públicos, auditores, peritos y demás especialistas estamos llamados a contribuir activamente a la transparencia, la integridad económica, la prevención del fraude y la protección de la confianza pública. Ante la evolución de los entornos digitales, este compromiso requiere ampliar nuestras competencias, fortalecer el juicio profesional e incorporar metodologías que permitan comprender, analizar y documentar operaciones cuya complejidad supera, en muchos casos, los procedimientos tradicionales de investigación financieras.

La tecnología blockchain y los criptoactivos representan, precisamente, uno de esos nuevos escenarios. Su estudio demanda una visión interdisciplinaria que integre la contabilidad, la auditoría, el derecho, la informática forense, el análisis de datos, el cumplimiento normativo y la investigación financiera. La identificación y trazabilidad de las transacciones, la preservación de la evidencia digital, la documentación de los hallazgos y la evaluación de los riesgos asociados constituyen capacidades esenciales para responder, con rigor técnico y responsabilidad ética, a las exigencias de esta nueva realidad.

Esta publicación aborda tales desafíos desde una perspectiva integral, reuniendo fundamentos tecnológicos, marcos normativos, criterios contables y tributarios, metodologías de auditoría forense, herramientas especializadas,

casos prácticos y orientaciones para el peritaje contable y la cooperación interamericana. Su alcance refleja la importancia de promover conocimientos que puedan ser aprovechados por profesionales de distintas disciplinas y jurisdicciones, respetando las particularidades normativas de cada país.

Como Presidente de la AIC, considero especialmente valioso que esta iniciativa sea fruto del trabajo colaborativo de especialistas de diversos países de las Américas. La integración de experiencias, conocimientos y perspectivas constituye una de las mayores fortalezas de nuestra Asociación y demuestra que los retos de la profesión no pueden abordarse de manera aislada. La cooperación técnica interamericana nos permite construir capacidades compartidas, enriquecer el debate profesional y avanzar hacia criterios de actuación cada vez más sólidos y consistentes.

Expreso, por tanto, mi reconocimiento a la Comisión Técnica Interamericana de Peritaje Contable y Auditoría Forense, a la Subcomisión responsable de la elaboración de esta obra, y a todos los profesionales, investigadores, académicos y colaboradores que aportaron sus conocimientos y experiencia para hacer posible esta primera edición. Su dedicación constituye una expresión concreta del valor del trabajo voluntario especializado y del compromiso con el desarrollo de nuestra profesión.

Es importante destacar que una obra de esta naturaleza no debe entenderse como un punto de llegada, sino como el inicio de un proceso permanente de aprendizaje, investigación y actualización. La evolución de los criptoactivos, las finanzas descentralizadas, la tokenización y las tecnologías emergentes exige revisar continuamente nuestros conocimientos, fortalecer la formación profesional y mantener una actitud crítica ante los nuevos riesgos y oportunidades. Este manual ofrece una base de referencia para avanzar en esa dirección, sin sustituir el juicio profesional ni la observancia de las normas y disposiciones aplicables en cada jurisdicción.

La AIC reafirma, mediante iniciativas como esta, su voluntad de impulsar una profesión contable preparada para el futuro, capaz de combinar innovación tecnológica con independencia de criterio, competencia técnica, objetividad y conducta ética. La incorporación de nuevas herramientas solo alcanza su verdadero valor cuando se orienta al interés público y contribuye a mejorar la calidad de la información, la transparencia de las operaciones y la confianza en las instituciones.

Invito a los profesionales de la contaduría pública, la auditoría forense, el peritaje, el derecho, la investigación financiera y las disciplinas tecnológicas a estudiar y aprovechar esta obra, compartir sus experiencias y contribuir a su perfeccionamiento. Que sus contenidos sirvan de apoyo para la formación de nuevas generaciones de especialistas y para el fortalecimiento de la colabo-

ración entre los organismos profesionales, las instituciones académicas y las autoridades competentes.

Con esta publicación, la Asociación Interamericana de Contabilidad renueva su compromiso con el conocimiento, la excelencia profesional y la integración de las Américas. Estamos convencidos de que una profesión que aprende innova y coopera está mejor preparada para afrontar los desafíos de su tiempo y para continuar siendo un referente de confianza al servicio de nuestras sociedades.

La tecnología transforma los medios; la ética, el conocimiento y la responsabilidad profesional siguen siendo los fundamentos de la confianzas.

Nelson Hahn
Presidente de la Asociación Interamericana de Contabilidad (AIC)

Mensajes del *Vicepresidente Asuntos Técnicos de la Asociación Interamericana de Contabilidad - AIC*

1. Una nueva realidad financiera, económica y tecnológica

La transformación digital ha y está redefiniendo todos los días la economía mundial y la forma en que las personas, las empresas y las instituciones realizan sus operaciones financieras. Los criptoactivos, las monedas digitales y la tecnología "blockchain" dan lugar a nuevas formas de inversiones, transferencia de valor, medición de valor, contratación y desarrollo de negocios, modificando progresivamente los mecanismos tradicionales de registro, control y supervisión de las operaciones económicas.

Esta evolución ofrece importantes oportunidades para la innovación y la eficiencia, pero también introduce escenarios de creciente y significativa complejidad para la profesión contable, la auditoría, la investigación financiera y la administración de justicia. Las características de los entornos digitales, la utilización de mecanismos criptográficos, la operación de plataformas descentralizadas y la posibilidad de efectuar transacciones transfronterizas plantean nuevos retos para la identificación de los participantes, la trazabilidad de los recursos tangibles y no tangibles, la determinación de su titularidad y la comprensión de las operaciones realizadas.

A estas circunstancias se suman los riesgos inherentes relacionados con el fraude financiero, el lavado de activos, la ocultación patrimonial y su forma de origen, la evasión de obligaciones tributarias y otros posibles usos ilícitos de los activos digitales. La investigación de estas operaciones requiere conocimientos que integren tecnología, contabilidad, finanzas, derecho y técnicas especializadas de análisis forenses.

En este entorno, la profesión contable enfrenta el desafío de evolucionar con mismo ritmo que las tecnologías que debe examinar. Tanto el auditor, como el perito contable ya no pueden limitar su actuación a los procedimientos tradicionales y convencionales de revisión documental y análisis de registros financieros; necesitan entender, comprender y evaluar los entornos blockchain, interpretar la evidencia digital y aplicar metodologías que permitan sustentar irrefutablemente sus conclusiones con rigor, independencia, objetividad y fundamento técnicos.

2. Fortalecer las capacidades profesionales y superar las brechas técnicas

La rápida evolución de los criptoactivos y de las tecnologías asociadas ha generado la necesidad de desarrollar conocimientos, metodologías y criterios técnicos que permitan afrontar adecuadamente los nuevos escenarios de auditoría e investigación financiera. La diversidad de marcos jurídicos y regulatorios, las diferencias en los tratamientos contables y tributarios, y la constante aparición de nuevas herramientas y modelos de negocio dificultan la aplicación de criterios uniformes y la ejecución de investigaciones técnicamente sustentadas.

Esta situación evidencia la importancia de disponer de orientaciones especializadas que articulen los fundamentos tecnológicos con las normas contables, tributarias y jurídicas, así como con los procedimientos de auditoría forense, la obtención y preservación de evidencia digital y la elaboración de informes periciales. La ausencia de una visión integral puede limitar la capacidad de los profesionales para identificar riesgos, reconstruir operaciones, documentar hallazgos y presentar conclusiones comprensibles, verificables y útiles para la toma de decisiones o para los procesos judiciales.

El desafío adquiere una dimensión particular en los países que forman parte de la Asociación Interamericana de Contabilidad, donde la cooperación profesional, el intercambio de experiencias y el conocimiento de las particularidades normativas de cada jurisdicción son fundamentales para responder a operaciones que, con frecuencia, superan las fronteras nacionales. En consecuencia, resulta útil e indispensable promover una formación especializada que contribuya a fortalecer las competencias de los contadores públicos, auditores, peritos, investigadores, académicos y demás profesionales vinculados con la prevención, detección e investigación de irregularidades financieras.

La necesidad no se limita al conocimiento de nuevas herramientas tecnológicas, también exige preservar los principios esenciales de la profesión: la ética, la independencia, un alto escepticismo profesional, la confidencialidad, la objetividad y el compromiso con el interés público. La tecnología puede ampliar las posibilidades de investigación, pero sus resultados deben interpretarse mediante criterios profesionales sólidos y procedimientos debidamente documentados.

3. Conocimiento integrado, metodología y aplicación profesional

Frente a esta realidad, la Asociación Interamericana de Contabilidad -AIC, a través de su Comisión Técnica Interamericana de Peritaje Contable y Auditoría Forense, presenta el “Manual de Auditoría Forense Especializado en Criptoacti-

vos, Moneda Digital y Blockchain", una nueva cobra de la Comisión que contribuye técnica y académicamente, y que orientada a fortalecer las capacidades profesionales y proporcionar una referencia integral para el estudio y la aplicación de procedimientos especializados en este campo emergentes.

Esta obra constituye una respuesta a la necesidad de vincular el conocimiento tecnológico con la práctica contable, la regulación, la auditoría y la investigación forense. Su estructura permite avanzar desde los fundamentos de los criptoactivos y la tecnología blockchain hasta el análisis de los marcos normativos internacionales, el tratamiento contable y tributario, los riesgos jurídicos y los delitos asociados. Sobre esta base, desarrolla metodologías de auditoría forense, procedimientos de investigación financiera digital, herramientas especializadas de análisis blockchain y medidas de ciberseguridad para la protección de los activos digitales.

En adición, el manual incorpora contenidos sobre: peritaje contable, prueba judicial, cooperación interamericana y recuperación de activos, complementados con casos de estudio, guías prácticas y un análisis de las tendencias emergentes de la auditoría forense. Este aporte de la Comisión busca facilitar no solo la comprensión conceptual de la materia, sino también la identificación de procedimientos y recursos que puedan orientar el trabajo profesional, de acuerdo con la legislación y las normas aplicables en cada país, la cual el lector debe abordarla y complementarlas.

Su alcance en los países de la región refleja la importancia de construir conocimiento de manera colaborativa, compartir experiencias y promover el desarrollo de capacidades técnicas que contribuyan a enfrentar desafíos comunes. En este sentido, la obra constituye una herramienta de consulta y formación para profesionales que requieren actualizar sus conocimientos y prepararse para intervenir en investigaciones relacionadas con activos digitales, y consulta para los estudiantes en las ramas de auditoria forense, peritaje y formación en áreas afines.

La Asociación Interamericana de Contabilidad reafirma, mediante esta publicación, su compromiso con el fortalecimiento de la profesión contable, la difusión del conocimiento y la preparación de sus profesionales frente a los cambios que transforman el entorno económico y financiero. Este manual representa un aporte al desarrollo de una auditoría forense capaz de integrar tecnología, conocimiento contable y responsabilidad profesional al servicio de la transparencia y la confianza públicas.

Invito a los lectores a estudiar este nutrido y sólido manual con una actitud crítica, reflexiva y orientada a la aplicación práctica. Que sus contenidos contribuyan a ampliar las competencias de nuestros profesionales, fortalecer la calidad de las investigaciones y consolidar la cooperación entre los países de Américas.

El juicio profesional no es reemplazado por ninguna herramienta tecnológica, más bien, la experiencia del profesional de una auditoría o un peritaje se fortalece con ella.

Idrián Estrella Silva
Vicepresidente Asuntos Técnicos
Asociación Interamericana de Contabilidad (AIC).

Mensaje del presidente de la Comisión Técnica Interamericana de Peritaje Contable y Auditoría Forense

Desde su creación, los criptoactivos (criptomoneda o criptodivisas) ha ido posicionándose de manera paulatina en algunos países, incluyendo las Americas. Naciones como Reino Unido en 2014 dio los primeros pasos ponderando el rol de este tipo de moneda en la economía y las posibles regulaciones a considerar. En el Salvador como es conocido acepto el Bitcoin como licitación legal, seguido de Cuba en 2021, no así en países como China y la Union Europea que prohibieron todo uso, transacción minada o negociación, con la intención de evitar fugas de capital y prohibir el anonimato a la hora de transferir criptomonedas.

Ante la realidad de un sistema que cada día se impone en los países, los delitos relacionados con criptoactivos, monedas digitales y blockchain, abordando principalmente fraudes, estafas piramidales y la naturaleza jurídica de estos activos, también se hacen notorio. Solo he de destacar las sentencias judiciales a nivel internacional y local que han condenado a personas, tal es el caso Cuarto Tribunal Colegiado del Distrito Nacional, sentencia febrero 2025 caso del Sr. Jairo González en República Dominicana precedente nacional por estafa masiva con monedas digitales; Tribunal: Corte Federal de Nueva York (marzo de 2024), caso Hechos: Sam Bankman-Fried fue declarado culpable de siete cargos de fraude y conspiración tras el colapso de la plataforma de intercambio de criptomonedas FTX, por el robo de aproximadamente 8,000 millones de dólares a los clientes; entre otros.

Lo expuesto ha motivado a la Comisión Técnica Interamericana de Peritaje Contable y Auditoría Forense de la AIC, dar los primeros pasos en materia de investigación pericial especializada en Criptoactivos, Moneda Digital y Blockehain, y conforma una subcomisión especial a cargo de destacados profesionales en la materia, con horas de prácticas, como es el caso de los doctores Juan Carlos Rivera Gómez – Colombia presidente, Abraham Siliezar Montes – El Salvador asesor técnico, Olga Jazmin Carrillo Rey – Colombia vicepresidenta y Marlene Roxana Almanza Cespedes – Bolivia secretaria, conjuntamente con un equipo de notables colegas de las Americas.

Como todo equipo de trabajo, se pudo observar los ejes principales en una gestión eficiente de cualquier proceso, proyecto o sistema de una organización (Integración, Coordinación y Comunicación), siendo palpable la armonía y con un propósito común.

De ahí nace el primer Manual de Auditoría Forense Especializado en Criptoactivos, Monedas Digital y Blockehain, Primera Edición, AIC. Para dar respuesta a un problema existente en materia de pericia especializada ante afectación al patrimonio de las personas como resultado de conducta que ya constituyen tipo penal en muchos países de las Americas. Invitamos a la comunidad disfrutar esta guía a fin de aportar claridad en los estrados judiciales de los países de las Americas.

Richard Gómez Jiménez

Presidente de la Comisión Técnica Interamericana de Peritaje Contable y Auditoria Forense de la AIC.

Palabras del Presidente de la Subcomisión a cargo del Manual de Auditoría Forence Especializado *en Criptoactivos, Moneda Digital y Blockchai, AIC*

Es un honor para mí ser parte de esta importante comisión en materia de la profesión contable y pues agradezco el voto de confianza al delegarme la presidencia de esta primera edición del Manual de Auditoría Forense Especializado en Criptoactivos, Moneda Digital y Tecnología Blockchain, como resultado del trabajo colaborativo de especialistas de diversas disciplinas comprometidos con el fortalecimiento de las capacidades profesionales y técnicas que hoy demanda la transformación digital de la economía global.

Expreso mi más profundo agradecimiento a cada uno de los integrantes de la subcomisión: investigadores, académicos, peritos contables, auditores forenses, abogados, ingenieros, analistas y demás profesionales. Asimismo, destaco el respaldo de la Dra. Olga Jazmín Carrillo Rey, Founder & Ceo del Anti- Fraud Institute- AFI Colombia, y de todos los profesionales de las ciencias económicas. Gracias a sus conocimientos, experiencia y dedicación, hicieron posible la construcción de este instrumento de referencia para la región de las Américas.

La constante evolución de los modelos de negocio, el surgimiento de nuevas formas de generación y transferencia de valor, así como la creciente adopción de activos virtuales sustentados en tecnologías blockchain, han planteado desafíos inéditos para las organizaciones, los sistemas regulatorios, las agencias del orden y los profesionales responsables de la prevención, detección, investigación y esclarecimiento de conductas que afectan la transparencia económica y financiera.

Los activos virtuales, comúnmente conocidos como criptomonedas o monedas digitales, representan uno de los avances tecnológicos más significativos de las últimas décadas. Su capacidad para facilitar operaciones transfronterizas, movilizar recursos de manera instantánea y generar nuevos ecosistemas económicos ha transformado la forma en que las personas, empresas y gobiernos interactúan dentro de los mercados globales. Sin embargo, estas mismas características pueden ser aprovechadas por estructuras criminales para ocultar activos, transferir recursos ilícitos, financiar actividades delictivas o dificultar los procesos tradicionales de rastreo.

Ante esta realidad, surge la necesidad de desarrollar metodologías, procedimientos divergentes y criterios técnicos que permitan a los profesionales comprender la naturaleza de estos activos, evaluar los riesgos asociados a su utilización y ejecutar procedimientos de auditoría forense que aporten elementos de juicio sólidos, verificables y científicamente sustentados a los procesos de investigación y administración de justicia.

Este manual constituye una respuesta inicial a esa necesidad. Su propósito es ofrecer una hoja de ruta práctica para quienes intervienen en procesos de auditoría forense, investigación financiera, análisis de inteligencia, peritaje especializado y apoyo técnico a las autoridades competentes.

Asimismo, busca promover la adopción de enfoques metodológicos fundamentados en estándares profesionales, técnicas de investigación reconocidas y buenas prácticas aceptadas por la comunidad técnico-científica Interamericana.

La presente obra no pretende ser un documento definitivo. Por el contrario, nace con la convicción de que el conocimiento relacionado con las tecnologías emergentes debe evolucionar permanentemente. Las dinámicas propias de los ecosistemas blockchain, las finanzas descentralizadas, la tokenización de activos y las nuevas formas de intercambio digital exigen una actualización constante de las metodologías de análisis e investigación.

Este primer ejemplar representa un hito para el hemisferio americano al consolidar experiencias reales de investigación, rastreo de transacciones, análisis de criptoactivos y construcción de evidencia digital aplicadas en diferentes contextos profesionales. Su contenido se encuentra fundamentado en casos prácticos, procedimientos técnicos, criterios de análisis y lecciones aprendidas derivadas de la experiencia de especialistas que han participado en investigaciones complejas y procesos de cooperación con autoridades judiciales y organismos de control.

Confiamos en que esta publicación contribuya significativamente al fortalecimiento de las capacidades de los profesionales de la contaduría pública, el derecho, la auditoría, la ingeniería de sistemas, la informática forense, la investigación financiera, el análisis criminal y demás disciplinas que desempeñan un papel fundamental en la protección de la integridad económica y financiera de nuestras sociedades.

Finalmente, deseamos que este manual se convierta en una herramienta de consulta permanente, un punto de encuentro para la cooperación técnica Interamericana y una referencia para futuras generaciones de profesionales llamados a enfrentar los retos que plantea la convergencia entre la tecnología, las finanzas y la administración de justicia.

La construcción de confianza en los ecosistemas digitales requiere conocimiento, rigor científico y compromiso ético. Este documento es una contribución a ese propósito común.

Mg. Juan Carlos Rivera Gómez

Presidente de la Subcomisión para el Diseño del Manual de Auditoría Forense Especializado en Criptoactivos, Moneda Digital y Blockchain de la AIC.

Palabras Asesor Técnico de la Subcomisión a cargo del Manual de Auditoría Forence Especializado *en Criptoactivos, Moneda Digital y Blockchai, AIC*

En torno a los criptoactivos persisten mitos y leyendas. Como profesionales, tenemos el deber de profundizar en el estudio y la comprensión de las tecnologías emergentes relacionadas con blockchain y los activos digitales. Por ello, nos proponemos desmitificar las zonas grises que suelen atribuírseles, través de esta guía metodología descrita en el primer Manual de Auditoría Forense Especializado en Criptoactivos, Moneda Digital y Blockchain.

El manual evidencia que estamos ante una tecnología totalmente trazable, auditable, inmutable y verificable en tiempo real.

Este manual marca un hito para la profesión contable del continente. Por primera vez, los contadores y auditores de las Américas cuentan con una referencia común para investigar, auditar y prevenir el fraude en un entorno financiero que evoluciona hacia los activos digitales. Haber contribuido con asistencia técnica a esta obra constituye un honor profesional y una responsabilidad que asumo con orgullo.

Valoro especialmente la visión de la AIC, a través de su Comisión Técnica Interamericana de Peritaje Contable y Auditoría Forense, al anticiparse a los desafíos que plantean Bitcoin y la tecnología blockchain. Destaco también el rigor y el espíritu colaborativo del equipo de trabajo: cada sesión de análisis permitió enriquecer el documento con experiencias de distintos países y fortalecer los lazos entre profesionales comprometidos con la transparencia financiera.

Reitero mi disposición a seguir colaborando en la difusión, la capacitación y la actualización de este manual, así como en futuras iniciativas que impulsen la modernización de la profesión contable en la región.

Abraham Siliezar Montes
Asesor Técnico de la Subcomisión para el Diseño del Manual de Auditoría Forense Especializado en Criptoactivos, Moneda Digital y Blockchain de la AIC.

OBJETIVO

Proporcionar a los profesionales de Iberoamérica que ejecutan labores en auditoría forense, contaduría pública, ciencias jurídicas, ingeniería, investigación financiera e informática forense, una guía metodológica y técnica para la identificación, análisis, rastreo, documentación e interpretación de evidencias asociadas con criptoactivos y tecnologías blockchain. Esto con el fin de contribuir al fortalecimiento de los procesos de prevención, detección, investigación judicial y administración de justicia en la región.

ALCANCE Y APLICACIÓN EN IBEROAMÉRICA

Constituye una guía técnica y metodológica orientada a fortalecer las capacidades de los profesionales de la contabilidad, la auditoría, el derecho, el cumplimiento normativo y la investigación financiera en los países de Iberoamérica. Su aplicación permite comprender, analizar, rastrear, documentar y valorar operaciones realizadas mediante tecnologías blockchain y activos virtuales, proporcionando herramientas para la obtención de indicios, evidencias y hallazgos con potencial valor probatorio. Asimismo, contribuye a la armonización de criterios técnicos entre las distintas disciplinas, fortaleciendo la prevención, detección e investigación de riesgos asociados a los criptoactivos, el cumplimiento regulatorio, la transparencia financiera y el apoyo a la administración de justicia en el contexto de la economía digital.

METODOLOGÍA

El presente Manual de Auditoría Forense Especializado en Criptoactivos, Moneda Digital y Blockchain ha sido estructurado en partes, capítulos y subcapítulos con el propósito de organizar de manera sistemática los conocimientos técnicos, científicos, contables, financieros, tecnológicos, regulatorios, tributarios, jurídicos y forenses asociados a los activos virtuales y las tecnologías blockchain.

Su construcción fue desarrollada por la Asociación Interamericana de Contabilidad (AIC), a través de la Comisión Técnica Interamericana de Peritaje Contable y Auditoría Forense, mediante la designación de una Subcomisión Especializada en Auditoría Forense de Criptoactivos, Moneda Digital y Blockchain, integrada por expertos de diversos países de las Américas con experiencia en auditoría forense, peritaje contable, investigación financiera, cumplimiento normativo, regulación de activos virtuales, informática forense y tecnología blockchain.

La metodología empleada se fundamentó en la construcción de conocimiento científico mediante la investigación documental, la lectura crítica y comparada de literatura académica especializada, normas profesionales, están-

dares internacionales, desarrollos regulatorios, estudios técnicos, experiencias prácticas de investigación y casos relacionados con la utilización de criptoactivos dentro de contextos económicos, financieros, administrativos, tributarios y penales. Este proceso permitió integrar conocimientos provenientes de las ciencias económicas, jurídicas y tecnológicas bajo un enfoque interdisciplinario y holístico.

Durante el desarrollo del manual fueron analizados los principales marcos normativos y técnicos internacionales, incluyendo las Normas Internacionales de Información Financiera (NIIF/IFRS), las Normas Internacionales de Auditoría (NIA) emitidas por el IAASB, las recomendaciones del Grupo de Acción Financiera (GAFI/FATF), los principios contenidos en el Código Internacional de Ética para Profesionales de la Contabilidad, así como diversas disposiciones regulatorias relacionadas con activos virtuales, prevención del lavado de activos, financiamiento del terrorismo, cumplimiento normativo y transparencia financiera.

De igual forma, se estudiaron las regulaciones nacionales de diversos países de Iberoamérica, identificando puntos de convergencia y diferencias en materia penal, fiscal, contable, financiera, tributaria y administrativa. Como resultado, las definiciones y procedimientos contenidos en este manual fueron construidos procurando una aplicabilidad amplia dentro de las distintas jurisdicciones de las Américas, respetando las particularidades normativas existentes en cada país.

La metodología también reconoce la influencia de los sistemas jurídicos predominantes en la región, especialmente aquellos sustentados en el Sistema Penal Oral Acusatorio, cuyos principios de legalidad, debido proceso, contradicción, imparcialidad judicial, presunción de inocencia, defensa técnica, carga probatoria, libertad de prueba y valoración racional de la evidencia constituyen referentes esenciales para la obtención, preservación, análisis y presentación de indicios, evidencias y hallazgos relacionados con activos virtuales y tecnologías blockchain.

Finalmente, el presente manual integra los fundamentos doctrinales previamente desarrollados por la AIC en el Manual de Procedimientos de Auditoría Forense y el Manual de Procedimientos de Peritaje Contable, ampliando su alcance hacia los nuevos desafíos planteados por la economía digital, la trazabilidad financiera descentralizada, la evidencia digital distribuida y la investigación forense especializada en criptoactivos, contribuyendo así al fortalecimiento de las capacidades profesionales de contadores públicos, auditores, abogados, oficiales de cumplimiento, investigadores financieros, peritos y operadores de justicia en los países de Iberoamérica.

GLOSARIO INICIAL DE TÉRMINOS TÉCNICOS

- A -

- Activo Digital: Representación electrónica de valor, derechos, información o propiedad susceptible de ser almacenada, transferida o gestionada mediante sistemas digitales. Incluye criptoactivos, monedas digitales, tokens y otros instrumentos basados en tecnologías de registro distribuido.
- Activo Virtual (AV): Representación digital de valor que puede comercializarse o transferirse digitalmente y utilizarse para pagos o inversiones, excluyendo monedas fiduciarias digitales emitidas por bancos centrales. Definición alineada con FATF-GAFI.
- Análisis Blockchain: Proceso técnico, financiero y forense mediante el cual se examinan registros distribuidos para identificar transacciones, relaciones entre direcciones, patrones de comportamiento, riesgos, beneficiarios reales y flujos de criptoactivos.
- Analista Cripto: Especialista encargado de efectuar trazabilidad de operaciones con activos virtuales, identificar origen y destino de fondos, determinar proveedores de servicios de activos virtuales y correlacionar operaciones blockchain con actividades del sistema financiero tradicional.
- Auditoría Forense Blockchain: Disciplina especializada que integra técnicas de auditoría, análisis financiero, informática forense e investigación criminal para detectar, documentar y presentar evidencia relacionada con operaciones realizadas mediante tecnología blockchain.

- B -

- Beneficiario Final Digital: Persona natural que ejerce control efectivo, propiedad o disposición sobre una billetera, dirección blockchain, cuenta en exchange o estructura descentralizada, independientemente de la titularidad formal registrada.
- Bitcoin (BTC): Primer criptoactivo descentralizado basado en tecnología blockchain, utilizado como reserva de valor, activo de inversión y medio de transferencia digital.
- Blockchain: Tecnología de registro distribuido que almacena información en bloques enlazados criptográficamente, permitiendo la inmutabilidad, trazabilidad y verificación descentralizada de las transacciones.
- Bridge (Puente Blockchain): Infraestructura tecnológica que permite transferir activos o información entre diferentes blockchains.

- Billetera Digital (Wallet): Aplicación, software, dispositivo o mecanismo que permite almacenar, administrar y transferir criptoactivos mediante el control de claves criptográficas.
- Billetera Custodiada: Wallet en la que las claves privadas son administradas por un tercero, normalmente un exchange o proveedor de servicios de activos virtuales.
- Billetera No Custodiada (Self-Hosted Wallet): Wallet controlada exclusivamente por el usuario, quien conserva la posesión de las claves privadas y la frase semilla.

- C -

- Cadena de Custodia Digital: Conjunto de procedimientos documentados que garantizan la integridad, autenticidad, trazabilidad y preservación de evidencias digitales relacionadas con criptoactivos.
- Chain Analysis: Metodología de inteligencia blockchain destinada a reconstruir flujos de activos virtuales, identificar entidades, detectar riesgos y asociar actividades digitales con personas, organizaciones o hechos investigados.
- Chainalysis Reactor: Herramienta especializada utilizada para visualizar redes transaccionales, identificar entidades vinculadas, establecer trazabilidad de fondos y generar evidencia útil para investigaciones financieras y auditorías forenses.
- Clave Privada: Elemento criptográfico secreto que permite controlar, firmar y autorizar transacciones asociadas a una dirección blockchain.
- Clave Pública: Identificador criptográfico visible que permite recibir activos virtuales dentro de una red blockchain.
- CoinJoin: Mecanismo de mezcla de transacciones diseñado para aumentar la privacidad y dificultar la trazabilidad blockchain.
- Contract Addres: Dirección blockchain que representa un contrato inteligente desplegado en una red determinada.
- Criptoactivo: Activo digital protegido mediante criptografía, cuyo uso, transferencia o propiedad puede registrarse en una blockchain o tecnología de registro distribuido.
- Criptomoneda: Tipo de criptoactivo diseñado principalmente como medio de intercambio, pago o reserva de valor dentro de ecosistemas digitales descentralizados.

- D -

- DAO (Decentralized Autonomous Organization): Organización gobernada mediante contratos inteligentes y procesos de votación descentralizados sin una administración central tradicional.
- DeFi (Finanzas Descentralizadas): Ecosistema de aplicaciones financieras construidas sobre blockchain que permiten servicios financieros sin intermediarios tradicionales.
- Dirección Blockchain: Identificador alfanumérico utilizado para enviar, recibir o almacenar activos virtuales dentro de una red blockchain.
- Due Diligence Blockchain: Proceso de verificación especializada para evaluar riesgos regulatorios, financieros, tecnológicos y reputacionales asociados al uso de criptoactivos.

- E -

- Exchange Centralizado (CEX): Plataforma administrada por una entidad que facilita la compra, venta y custodia de criptoactivos.
- Exchange Descentralizado (DEX): Protocolo basado en contratos inteligentes que permite intercambios de activos digitales sin intermediarios centralizados.
- Evidencia Digital Blockchain: Conjunto de registros verificables contenidos en una blockchain que pueden ser utilizados con fines probatorios.

- F -

- Fee o Comisión de Red: Pago realizado a validadores o mineros por procesar y registrar transacciones dentro de una blockchain.
- Forense Blockchain: Disciplina aplicada a la identificación, preservación, análisis y presentación de evidencia derivada de registros blockchain.
- Frase Semilla (Seed Phrase): Secuencia de palabras que permite recuperar o recrear una billetera y obtener acceso a los activos asociados.

- G -

- Gobernanza Descentralizada: Sistema de toma de decisiones basado en reglas automáticas, contratos inteligentes o votaciones comunitarias.
- Gas: Unidad utilizada para medir el costo computacional de operaciones ejecutadas en determinadas blockchains como Ethereum.

- H -

- Hash: Identificador criptográfico único utilizado para verificar información, bloques y transacciones.

- Hash Transaccional (TXID): Código único que identifica una transacción específica dentro de una blockchain.

- K -

- KYC (Know Your Customer): Procedimiento de debida diligencia utilizado por entidades financieras y PSAV para identificar y verificar usuarios.

- L -

- Lavado de Activos mediante Criptoactivos: Proceso mediante el cual recursos ilícitos son ocultados, convertidos o transferidos utilizando tecnologías blockchain, exchanges, mixers o protocolos DeFi.
- Layer 1: Blockchain principal que proporciona infraestructura base para transacciones y contratos inteligentes.
- Layer 2: Soluciones tecnológicas diseñadas para escalar blockchain mediante reducción de costos y aumento de velocidad.

- M -

- Metaverso: Entorno virtual interoperable donde pueden existir activos digitales, identidades digitales y economías basadas en blockchain.
- Mezclador (Mixer o Tumbler): Servicio orientado a ocultar el origen o destino de activos virtuales mediante la mezcla de múltiples transacciones.
- Minería: Proceso de validación de transacciones y emisión de nuevas unidades monetarias en blockchains basadas en Proof of Work.
- Moneda Digital de Banco Central (CBDC): Representación digital oficial de una moneda soberana emitida por una autoridad monetaria.

- N -

- NFT (Non-Fungible Token): Activo digital único e irrepetible registrado en blockchain que representa propiedad de un objeto físico o digital.

- P -

- PSAV (Proveedor de Servicios de Activos Virtuales): Entidad o persona que realiza actividades relacionadas con intercambio, custodia, transferencia o administración de activos virtuales.
- Proof of Stake (PoS): Mecanismo de consenso basado en la participación económica de validadores.
- Proof of Work (PoW): Mecanismo de consenso basado en capacidad computacional para validar bloques.

- R -

- Riesgo Blockchain: Probabilidad de que una dirección, entidad o transacción esté vinculada con actividades ilícitas, sanciones internacionales o incumplimientos regulatorios.
- Riesgo de Contraparte Digital: Posibilidad de pérdidas derivadas del incumplimiento de un exchange, protocolo DeFi o custodio.

- S -

- Smart Contract: Programa autoejecutable desplegado en blockchain que ejecuta automáticamente condiciones previamente definidas.
- Stablecoin: Criptoactivo diseñado para mantener estabilidad de valor respecto a una moneda fiduciaria, materia prima u otro activo de referencia.
- Staking: Proceso mediante el cual activos virtuales son bloqueados para participar en la validación de una red blockchain a cambio de recompensas.

- T -

- Token: Representación digital de derechos, activos, servicios o valor emitida sobre una blockchain existente.
- Tokenización: Proceso mediante el cual un activo físico o intangible se representa digitalmente mediante tokens registrados en blockchain.
- Trazabilidad On-Chain: Capacidad de reconstruir movimientos históricos de activos virtuales utilizando la información pública registrada en blockchain.
- Travel Rule: Requisito regulatorio internacional impulsado por FATF-GAFI que exige intercambio de información entre proveedores de servicios de activos virtuales.

- U -

- Utility Token: Token diseñado para otorgar acceso a bienes, servicios o funcionalidades específicas dentro de una plataforma.

- W -

- Wallet Address: Dirección pública utilizada para recibir o enviar activos digitales dentro de una blockchain.
- Wallet Screening: Proceso automatizado para evaluar riesgos asociados a direcciones blockchain mediante herramientas analíticas especializadas.

PARTE I

Fundamentos Generales de los Criptoactivos y la Tecnología Blockchain

1 INTRODUCCIÓN A LOS CRIPTOACTIVOS Y ACTIVOS VIRTUALES

1.1 Evolución del dinero y transformación digital financiera

Origen del intercambio

A lo largo de la historia, el ser humano ha tenido la necesidad de realizar anotaciones y cuantificaciones de la vida cotidiana. A medida que este proceso de desarrollo ha avanzado, también lo han hecho las necesidades, lo cual ha llevado a buscar mecanismos eficientes que permitan generar operaciones de intercambio con rapidez.

En la antigüedad, el trueque se volvió primordial: cada persona producía aquello que sabía producir mejor. Sin embargo, a medida que las sociedades crecieron, este sistema generó una serie de problemas y dificultades, tales como la indivisibilidad, la falta de coincidencia de preferencias y la intertemporalidad.

Con el nacimiento del concepto de propiedad privada, el trueque se consolidó como un mecanismo de intercambio de bienes entre pares, distinto de la compra y venta, pero que igualmente implicaba un cambio de propiedad y una transacción comercial cuyo objetivo era satisfacer necesidades.

No obstante, el desarrollo de la humanidad redefinió la forma y el método de los intercambios. Para que estos se generaran, era necesario contar con símbolos generalizados, los cuales debían cumplir con ciertas características: durabilidad, portabilidad, divisibilidad, verificabilidad y escasez.

En ese orden, la primera acuñación de moneda en la historia mundial fue creada en el Reino de Lidia actualmente territorio de Turquía durante el siglo VII a. C. Su material estaba hecho de una aleación natural de oro y plata, y llevaba grabado el diseño de una cabeza de león que funcionaba como sello real; este sello sirvió para estandarizar el valor del dinero y formalizar el comercio. Posteriormente, los imperios griego y romano adoptarían el mismo modelo.

Dinero institucional

Banca moderna

En la cuna del Renacimiento surge también la banca moderna, aproximadamente en el año 1400. Uno de los mecanismos clave para su desarrollo fue el principio de la partida doble.

La ciudad de Florencia vio el nacimiento de la estructura bancaria, que introdujo importantes cambios vigentes hasta hoy en día, como la letra de cambio mecanismo mercantil que establecía una orden de pago entre comerciantes, bancos y clientes, las cartas de crédito una de las innovaciones financieras más importantes de la historia y el uso de filiales para facilitar el intercambio comercial.

Patrón oro

La naturaleza ha dispuesto de metales preciosos escasos, como el oro y la plata. No existe una fecha determinística sobre el momento en que estos metales se establecieron como medio de cambio; sin embargo, comenzaron a tener un flujo considerable muchos siglos antes de la era cristiana, consolidándose con el paso del tiempo como depósito de valor.

El patrón oro fue un sistema monetario que fijaba el valor de cada unidad monetaria en relación con una determinada cantidad de oro. Los bancos centrales de los países que adoptaron este sistema emitían moneda según las reservas de oro de que disponían. Se trató de un sistema monetario internacional que funcionó gracias a la cooperación de los países que lo adoptaron y que, mientras estuvo en uso, facilitó el comercio internacional y limitó las políticas económicas aislacionistas entre países, entre 1870 y 1914.

Los conflictos bélicos y geopolíticos llevaron a reestructurar el patrón oro entre 1914 y 1930; al no poder vincular sus monedas directamente al oro, se estableció el patrón de lingote de oro.

Acuerdo de Bretton Woods

Según el Instituto de Estudios Bursátiles, el Acuerdo de Bretton Woods tuvo como propósito diseñar un sistema económico de posguerra que promoviera la coordinación internacional, la reconstrucción y el crecimiento; para ello se crearon el Fondo Monetario Internacional (FMI) y el Grupo del Banco Mundial (GBM).

En el Acuerdo se estableció que las monedas se vincularían al oro como estándar de referencia, utilizado en los cálculos por todos los países participantes. La tasa oficial fue de 35 dólares estadounidenses por onza troy de oro, debido a que Estados Unidos poseía las mayores reservas de oro y podía

garantizar el cambio de su moneda nacional por el metal precioso. Dada la influencia de Gran Bretaña, su moneda, la libra esterlina, fue reconocida como una moneda de reserva adicional.

Abandono del Acuerdo de Bretton Woods

Dado que el oro es un recurso escaso, la convertibilidad de las monedas en función de las reservas de oro no resultaba sostenible en el tiempo. Por ello, en 1971 Estados Unidos definió una nueva política monetaria orientada a reducir la tasa de desempleo.

El abandono del Acuerdo de Bretton Woods convirtió al dólar en dinero fiduciario, es decir, en una moneda no respaldada por oro y cuyo valor proviene de la confianza del sector económico. Los efectos de este cambio se materializaron, entre otros episodios, en la crisis económica de 2007-2008.

Revolución digital

En 1950 surge la primera tarjeta de crédito, Diners Club. En la década de 1990 se realiza la primera compra de comercio electrónico y surgen pasarelas de pago como PayPal.

En plena crisis económica, a finales de 2008 nace el primer protocolo de finanzas descentralizadas: Bitcoin, que cumple con todas las condiciones de un símbolo de valor, es decir, con las características de durabilidad, portabilidad, divisibilidad, verificabilidad y escasez.

El valor y la comunicación de valor

A principios de 2009, Satoshi Nakamoto minó el primer bitcoin, conocido como el "bloque génesis". En la programación de este primer bloque figuraba el texto *"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"*, en referencia a un titular del periódico británico The Times publicado en esa fecha, lo cual se considera generalmente como prueba del momento en que se minó el primer bitcoin. Otros interpretan que este mensaje también señalaba el deterioro de la infraestructura financiera del mundo moderno y la necesidad de un nuevo camino a seguir.

Bitcoin representa el salto de la abstracción a la utilidad: el nacimiento de un mercado descentralizado y el valor de un consenso dinámico.

Entender cómo funciona el dinero es fundamental para comprender los activos digitales. El dinero tradicional, como el efectivo o el dinero en cuentas bancarias, se basa en un sistema centralizado en el que los bancos y los gobiernos regulan la emisión y las transacciones. El fenómeno evolutivo permite elegir los símbolos que funcionan mejor y desechar los que no

funcionan. Para que un símbolo sea considerado un buen símbolo de valor, debe cumplir tres funciones: unidad de cuenta, medio de pago y reserva de valor.

Los intercambios y los símbolos generan oferta y demanda: cuando la cantidad de símbolos supera la de los intercambios reales que respaldan, se generan desequilibrios en su valor.

Esta es la primera vez en la historia en que la tecnología permite contar con una base de datos confiable entre dos personas que no se conocen ni confían entre sí, sin necesidad de un intermediario. Esto cambia el mundo para siempre.

En la actualidad, la accesibilidad de la tecnología a través del uso generalizado de teléfonos móviles facilita la inclusión financiera y revoluciona la gestión de las finanzas personales. Los cambios fundamentales se orientan en tres sentidos: la evolución de la partida doble a través de la blockchain, el acceso generalizado a dispositivos conectados a internet y las redes distribuidas, es decir, redes que no requieren una contraparte central. Estos elementos clave se materializan a través de Bitcoin.

Podríamos identificar una línea de tiempo de diversos conceptos que permitieron que al día de hoy tengamos un ecosistema robusto para el tratamiento de activos virtuales.

Año	Desarrollo	Aporte al futuro ecosistema de activos virtuales
1981	David Chaum – privacidad y comunicaciones digitales	Base conceptual de comunicaciones y pagos con privacidad
1982	**David Chaum – Blind Signatures**	Firmas ciegas y pagos electrónicos no rastreables
1983	Publicación de *Blind Signatures for Untraceable Payments*	Formalización académica del concepto
	DigiCash/eCash	Intento práctico de dinero electrónico criptográfico
1992	Dwork y Naor – *Proof of Work*	Introducción de mecanismos de trabajo computacional para limitar abuso
1997	Adam Back – **Hashcash**	Prueba de trabajo basada en funciones hash
1998	Wei Dai – **b-money**	Dinero electrónico distribuido y pseudónimo
	Nick Szabo – **Bit Gold**	Escasez digital + proof-of-work + registro de propiedad

Año	Desarrollo	Aporte al futuro ecosistema de activos virtuales
2004	Hal Finney – **RPOW**	Tokens basados en prueba de trabajo reutilizable
2008	Satoshi Nakamoto – **Bitcoin White Paper**	Integración de varias ideas en dinero electrónico P2P
2009	Lanzamiento de Bitcoin	Primera implementación funcional de una red monetaria P2P basada en blockchain/PoW

Fuente: Elaboración para la estructura histórica de este manual

1.2 Concepto de criptoactivos

Si bien no existe una forma estándar para definir el concepto de criptoactivos, el término generalmente aceptado los describe como una forma de moneda digital o virtual que opera independientemente de los sistemas bancarios tradicionales. Utiliza tecnología criptográfica para asegurar las transacciones y controlar la creación de nuevas unidades. A diferencia de las monedas convencionales, las criptomonedas no dependen de una autoridad central emisora o reguladora; en cambio, emplean un sistema descentralizado que registra las transacciones y mantiene un libro mayor transparente.

De acuerdo con el Grupo de Acción Financiera de Latinoamérica (GAFILAT), un activo virtual es una representación digital de valor que puede comercializarse o transferirse digitalmente y que puede utilizarse para pagos o inversiones.

Sin perjuicio de las definiciones vigentes en otras jurisdicciones de Iberoamérica y para efectos estrictamente prácticos y analíticos de este manual, se adoptará la definición contenida en el artículo 3 de la Ley de Emisión de Activos Digitales de El Salvador, por reunir el concepto técnico y legal de la siguiente manera:

"Un activo digital es una representación digital que puede almacenarse y transferirse electrónicamente, utilizando un sistema de Tecnología de Registro Distribuido, o tecnología similar o análoga, en la cual los registros se encuentran enlazados y cifrados para proteger la seguridad y privacidad de las transacciones. Como característica esencial, los activos digitales pueden ser poseídos, intercambiados, transferidos, negociados y promovidos por personas naturales y jurídicas. Los activos digitales no se consideran títulos valores y, por lo tanto, no les serán aplicables las disposiciones referentes a los títulos valores."

1.3 Tipología de activos virtuales

Si bien no existe una clasificación única y universalmente aceptada de los activos digitales, la clasificación generalmente adoptada en el ecosistema se define de la siguiente manera.

En el ecosistema de activos digitales existen miles de proyectos únicos, cada uno con funcionalidades y tecnologías distintas. La gran mayoría de estos protocolos cuenta con sus propias monedas digitales, las cuales, para efectos de este manual, se tipifican de la siguiente forma:

Tabla No. 1

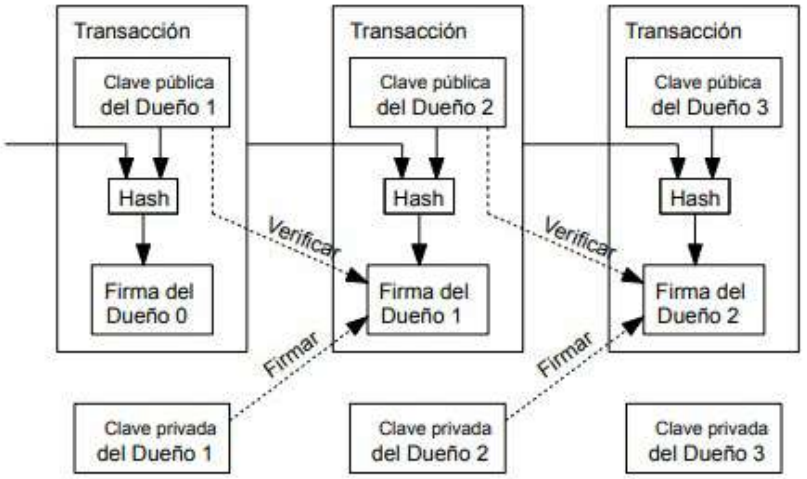
Tipología	Función Principal	Ejemplos Clave
Criptomonedas nativas (Layer 1)	Activos de redes descentralizadas; funcionan como incentivo de seguridad (pago de gas) y reserva de valor.	Bitcoin (BTC), Ethereum (ETH)
Stablecoins (monedas estables)	Vinculadas a la paridad con una moneda fiduciaria mediante colateralización (fiduciaria, cripto o algorítmica).	USDT, USDC, DAI
Security tokens (tokens de valor)	Representaciones digitales de activos financieros tradicionales (acciones, deuda, bienes raíces) bajo contratos inteligentes.	Acciones tokenizadas, RWA (*Real World Assets*)
Utility & governance tokens	Otorgan derechos de voto en protocolos DeFi o acceso a servicios específicos dentro de aplicaciones descentralizadas (dApps).	Uniswap (UNI), Chainlink (LINK)
Tokens no fungibles (NFT)	Unidades criptográficas que representan la propiedad única, irrepetible y demostrable de un activo específico.	Arte digital, identidades en cadena, activos de metaverso

Fuente: construcción propia y busca la diferenciación de los diversos términos y/o definiciones.

Bitcoin

De acuerdo con el *White Paper* de Bitcoin, este se define como “un sistema de efectivo electrónico usuario a usuario” (*peer-to-peer electronic cash system*) basado en pruebas criptográficas, que permite a las partes interesadas realizar transacciones sin necesidad de la intervención de un tercero. Es una red blockchain pública y descentralizada que registra de forma inmutable las entradas y salidas de valor.

Imagen No. 1



Fuente: Cadena de firmas digitales en una transacción de Bitcoin.

Tabla No. 2

1. ARQUITECTURA Y FUNDAMENTOS CRIPTOGRÁFICOS
• **Red Peer-to-Peer (P2P):** Infraestructura descentralizada de nodos interconectados, sin servidores centrales ni entidades fiduciarias intermediarias. • **Criptografía asimétrica:** Uso de pares de claves pública y privada. La clave privada genera firmas digitales indiscutibles que permiten autorizar y transferir la propiedad de los activos. • **Funciones hash (SHA-256):** Algoritmo criptográfico unidireccional que asegura la inmutabilidad de los bloques encadenados y garantiza la integridad de toda la red.

Tabla No. 3

2. CADENA DE TRANSACCIONES Y VALIDACIÓN CRIPTOGRÁFICA
• **Modelo de propiedad:** Una moneda se define conceptualmente como una cadena de transacciones digitales firmadas de manera digital. • **Verificación de propietarios:** Cada propietario transfiere el activo firmando digitalmente un hash de la transacción previa y la clave pública del siguiente propietario, añadiendo esta información al final de la moneda. • **Resolución del doble gasto:** El sistema incorpora marcas de tiempo (*timestamps*) y un registro público distribuido, el cual es validado permanentemente mediante un mecanismo de consenso descentralizado para evitar que un mismo activo sea gastado más de una vez.

Tabla No. 4

3. MECANISMO DE CONSENSO: PRUEBA DE TRABAJO (PoW)
• **Minería computacional:** Proceso de resolución por fuerza bruta de hashes, orientado a encontrar un objetivo (*target*) que asegure y valide el nuevo bloque. • **Inmutabilidad histórica:** Modificar un bloque pasado requiere recalcular todo el trabajo computacional posterior de la red, lo que otorga una seguridad criptográfica sin precedentes. • **Suministro algorítmico:** Emisión monetaria programada y descentralizada, limitada estrictamente a un máximo de **21 millones de unidades**, con reducciones periódicas a la mitad (*halving*) cada 210 000 bloques.

Bitcoin creó un sistema descentralizado y finito, en el que la emisión de monedas está prediseñada en 21 millones de unidades, divisibles cada una en 100 millones de partes denominadas satoshis, en honor a su creador. Al tratarse de dinero programable, su protocolo establece un suministro inalterable por diseño.

Ethereum

La segunda criptomoneda más importante del ecosistema es Ethereum, una red blockchain pública y descentralizada que opera como una computadora global compartida. A diferencia de Bitcoin, concebido principalmente para transferir valor entre pares, Ethereum fue diseñado como una plataforma programable donde cualquier persona puede escribir y ejecutar código directamente sobre la red, sin intermediarios.

Estos programas se denominan contratos inteligentes (*smart contracts*) y constituyen la base de todo el ecosistema contemporáneo de finanzas descentralizadas (DeFi), tokens no fungibles (NFT), monedas estables y protocolos abiertos.

Desde la perspectiva de la trazabilidad, esto resulta fundamental: en Ethereum no solo se registran transferencias de valor, sino también la ejecución de lógica programada. Cada acción deja un registro permanente e inmutable en la cadena.

Componentes clave de Ethereum:

- **Máquina Virtual de Ethereum (EVM):** Es el motor computacional que ejecuta los contratos inteligentes. Funciona como una supercomputadora virtual que corre de forma idéntica y simultánea en miles de nodos alrededor del mundo. Cuando un usuario interactúa con un contrato, todos los nodos ejecutan exactamente el mismo código y llegan al mis-

mo resultado, garantizando la descentralización y la inmunidad frente a manipulaciones.

- **Ether (ETH):** Es la criptomoneda nativa de la red y cumple dos funciones esenciales: actúa como reserva y activo de valor transferible, y funciona como el combustible (*gas*) necesario para pagar el costo de computación y ejecución de operaciones en la red (desde transferencias simples hasta interacciones complejas en DeFi).
- **Mecanismo de consenso (Proof of Stake / Prueba de Participación):** A diferencia de Bitcoin, el protocolo de Ethereum utiliza un sistema donde los validadores bloquean 32 ETH bajo un esquema de *staking*, ejecutando software especializado para certificar bloques y asegurar la red a cambio de recompensas algorítmicas.

Monedas estables (*stablecoins*)

Estas criptomonedas se caracterizan por mantener una paridad de valor de uno a uno (1:1) respecto a un activo subyacente, habitualmente una moneda fiduciaria tradicional como el dólar estadounidense. Combinan la eficiencia, inmediatez y portabilidad propias de la tecnología blockchain con mecanismos de estabilidad de precios, lo que las ha convertido en el instrumento financiero digital más utilizado para el comercio global y las remesas transfronterizas.

Tabla No. 5

Característica	Tether (USDT)	USD Coin (USDC)	DAI (DAI)
Tipo de modelo	Respaldada por dinero fiduciario.	Respaldada por dinero fiduciario.	Respaldada por criptoactivos.
Reservas y respaldo	Dólares físicos, bonos del Tesoro de EE. UU. y equivalentes de efectivo líquido.	Efectivo y bonos del Tesoro a corto plazo, auditados mensualmente por firmas públicas.	Contratos inteligentes con sobrecolateralización (ETH, WBTC) que absorben la volatilidad.
Entidad emisora	Tether Limited.	Consorcio Circle / Coinbase.	MakerDAO (gobernanza descentralizada).
Ventaja principal	Es la *stablecoin* más antigua, con mayor liquidez y volumen de comercio a nivel mundial.	Ampliamente preferida por instituciones y aplicaciones DeFi por su transparencia y cumplimiento regulatorio.	Completamente descentralizada y gestionada por código informático, lo que mitiga el riesgo de censura externa.

Particularmente en el caso de DAI, por tratarse de una moneda de gobernanza descentralizada y gestionada mediante contratos inteligentes, en un proceso de auditoría forense representa un activo de mayor complejidad en materia de seguridad y trazabilidad. Asimismo, existen otras monedas orientadas específicamente a la privacidad, como Monero y ZCash.

Monedas algorítmicas

Buscan mantener una vinculación de valor sin garantía colateral directa, mediante el uso de contratos inteligentes que ajustan algorítmicamente la oferta en función de la demanda del mercado. La estabilidad de precios de este tipo de monedas no siempre ha resultado fiable.

Es importante reconocer que estas monedas conllevan riesgos significativos, incluidos los riesgos operativos y de emisión. El respaldo colateral o el activo subyacente de estos tokens podría estar en manos de instituciones que llegasen a declararse insolventes, y las *stablecoins* algorítmicas podrían colapsar debido a errores de diseño u otros fallos sistémicos.

Initial Coin Offering (ICO)

Las ofertas iniciales de monedas (*Initial Coin Offerings*, ICO) constituyen un método de financiación colectiva mediante el cual un proyecto de criptomonedas vende tokens digitales en una fase temprana a cambio de capital, lo que permite obtener financiamiento directamente sin pasar por los filtros del sistema financiero tradicional.

Token

De acuerdo con el marco normativo de referencia, un token se define como un activo digital utilizado como unidad de cuenta dentro de una red, basado en la Tecnología de Registro Distribuido o una tecnología similar o análoga.

Los tokens están estrechamente vinculados a los contratos inteligentes, definidos legalmente como:

"Un programa informático, el cual utiliza la tecnología de registro distribuido o una similar o análoga, y que se implementa cuando ciertas condiciones predeterminadas se cumplen; se utiliza típicamente para automatizar la ejecución de un acuerdo, de manera que todos los participantes puedan tener certeza del resultado, sin necesidad de un intermediario. Según el acuerdo entre las partes, dichos programas pueden ser autoejecutables, ejecutados judicialmente o ejecutados de forma combinada [...]".

Diferencias entre criptomonedas, tokens y monedas digitales

- **Criptomoneda nativa (Layer 1):** Es el activo propio de una red blockchain, es decir, el "combustible" que la propia red crea y reconoce como dinero programable para funcionar. Bitcoin (BTC) es la moneda nativa de la red Bitcoin; *ether* (ETH) es la moneda nativa de la red Ethereum. Estas monedas existen porque la propia red las emite, las gestiona y las necesita para operar; no dependen de ninguna entidad externa ni de ningún contrato adicional: son la red.
- **Token:** Es un activo construido sobre una red ya existente. No es la moneda nativa de esa red, sino un activo creado en una capa superior, utilizando la infraestructura de la blockchain como plataforma. Para que un token exista, es indispensable que se haya desplegado en la red un programa especial llamado contrato inteligente, que define las reglas de emisión, suministro y transferencia. Un ejemplo claro es la moneda estable USDT: un token que transita sobre Ethereum o sobre otras redes, pero que no constituye la moneda nativa de ninguna de ellas.

Implicaciones para el análisis forense y la trazabilidad

Para un analista forense, esta distinción resulta sumamente importante. Al observar una transacción en los distintos exploradores de bloques (*block explorers*), la forma en que la red registra el movimiento de una moneda nativa es estructuralmente diferente de la forma en que registra el movimiento de un token.

Un ejemplo relevante en materia de trazabilidad es que USDT existe simultáneamente en la red Ethereum, en la red Tron y en BNB Smart Chain, es decir, en distintas cadenas compatibles con la Máquina Virtual de Ethereum o equivalentes. Mantiene la misma promesa de valor de uno a uno con la moneda fiduciaria y es emitido por la misma compañía, pero se implementa mediante contratos diferentes en cada red:

- En Ethereum, USDT opera como un contrato inteligente con una dirección específica.
- En Tron, opera mediante otro contrato con una dirección distinta en otra infraestructura de red.

Se trata de implementaciones separadas, coordinadas por el emisor, que mantienen equivalencia de valor entre sí, pero que técnicamente son contratos independientes ejecutados en cadenas independientes.

Análisis estructural: transferencias nativas frente a contratos inteligentes

Tabla No. 6

Comparativa técnica: Envío de moneda nativa vs. Envío de tokens

Dimensión del análisis	Envío de moneda nativa (Ej. Bitcoin / Ether)	Envío de tokens (Ej. USDT)
Naturaleza de la operación	Transacción directa y nativa de valor dentro del estado global de la red.	Ejecución de un programa informático (contrato inteligente del token dentro de la red).
Mecánica de registro	La red actualiza directamente el saldo: la dirección emisora reduce su balance y la receptora lo aumenta.	La dirección emisora llama al contrato indicando la transferencia; el contrato valida las reglas y actualiza su registro interno.
Intermediarios y programas	Inexistentes. La red procesa y actualiza sus registros base sin requerir código intermedio.	Involucra la ejecución directa de la lógica programada en el contrato inteligente del token.
Rol del activo nativo (ETH/BTC)	El activo nativo es el valor que se transfiere directamente de una dirección a otra.	El activo nativo no se transfiere como valor principal; únicamente se consume como combustible (*gas*) para pagar la ejecución de la transacción.
Resultado estructural	Cambio directo en el balance de cuentas nativas registrado de forma permanente en el bloque.	Modificación exclusiva en el estado interno de saldos gestionado por el programa o contrato inteligente.

Ecosistema blockchain y economía digital descentralizada

El dinero debe cumplir con su función principal, que consiste en poner precio a las cosas, pero no genera valor por sí mismo: lo que genera valor es el intercambio. Al analizar las distintas formas del dinero, se observa que el dinero considerado "bueno" debe cumplir con las características propias de los símbolos de valor.

En consecuencia, el dinero digital, al regirse por reglas de consenso, permite programar el dinero, lo que abre posibilidades para múltiples usos. A través de las finanzas descentralizadas, ya es posible representar un activo real mediante un activo subyacente.

Sobre esta arquitectura se ha desarrollado un ecosistema de finanzas descentralizadas (DeFi) que mejora los servicios financieros tradicionales mediante aplicaciones descentralizadas (*dApps*) y contratos inteligentes, siendo Ethereum la principal cadena de bloques utilizada para este propósito.

Por otra parte, la tokenización se ha convertido en un mecanismo de financiamiento empresarial orientado a estandarizar el uso de blockchain en los

sectores público, financiero, energético y de salud, consolidando lo que se denomina la nueva economía digital descentralizada.

A través de la tokenización y las finanzas descentralizadas, ya es posible la incorporación de materias primas agrícolas (*agrocommodities*), como la soja en Brasil, o la tokenización ganadera en los Países Bajos.

Riesgos y oportunidades para la contaduría pública

En la actualidad, los activos digitales ya no son el futuro: representan la realidad económica presente. Por lo tanto, el mayor desafío para los profesionales de la contaduría pública consiste en comprender cómo funcionan, cómo se clasifican, cuál es la anatomía de sus transacciones, cuál es la arquitectura de la blockchain y el papel determinante que desempeñan los contratos inteligentes.

Los profesionales de la contaduría pública, en sus distintas áreas de ejercicio, son responsables del registro, la preparación y la validación de los informes financieros de las entidades. Por ello, resulta indispensable demostrar la existencia de trazabilidad y, en consecuencia, de un protocolo auditable y verificable.

Si bien es cierto que, al referirnos a los activos digitales, de manera implícita solemos asociarlos con riesgos, evasión fiscal y lavado de activos, también lo es que, a través de las diversas herramientas de la auditoría forense, existe la capacidad legal, técnica y tecnológica para determinar el uso y el propósito de los activos digitales, así como su papel frente a las finanzas descentralizadas.

Por otra parte, las entidades responsables de la emisión de las Normas Internacionales de Contabilidad reconocen a los activos digitales como intangibles. No obstante, se requiere una evaluación técnica profunda para reconocer que estos activos ya constituyen medios de pago transfronterizos y que, en determinados países, ya son objeto de tratamientos o exclusiones tributarias específicos de acuerdo con los mecanismos legales aplicables en sus jurisdicciones.

Frente a estos retos, el ecosistema de activos digitales amplía de forma concreta el campo de acción del contador público. La tecnología no sustituye al profesional contable, sino que exige la incorporación de nuevas competencias en auditoría digital, regulación basada en riesgos, ciberseguridad y análisis de datos financieros descentralizados.

2 FUNDAMENTOS TECNOLÓGICOS DE BLOCKCHAIN

Objetivo del capítulo

Dotar al contador público, auditor interno y perito contable forense iberoamericano de un marco técnico-conceptual suficiente para comprender la arquitectura tecnológica subyacente a los criptoactivos y la moneda digital, de modo que pueda planificar procedimientos de auditoría, preservar evidencia digital con integridad probatoria y evaluar riesgos de lavado de activos y financiamiento del terrorismo (LA/FT) en entornos basados en tecnología de registro distribuido (DLT).

2.1 Conceptos básicos de blockchain

La tecnología blockchain constituye una especie dentro del género más amplio de las tecnologías de registro distribuido (*Distributed Ledger Technology*, DLT). Desde la perspectiva del perito contable forense, no interesa la blockchain como curiosidad informática, sino como un nuevo soporte de la prueba documental y de la evidencia digital: un libro mayor (*ledger*) replicado, sincronizado y según su diseño con resistencia práctica a la alteración retroactiva de los registros que contiene.

Esta característica transforma la manera en que se practican los procedimientos clásicos de auditoría de existencia, integridad, exactitud y corte, obligando a un tránsito conceptual desde el "rastro documental" en papel o en bases de datos centralizadas hacia el "rastro criptográfico" verificable matemáticamente.

En términos funcionales, una blockchain es una base de datos distribuida entre múltiples participantes (*nodos*) que mantienen copias idénticas o eventualmente consistentes de un mismo registro, sin que exista una autoridad central única con potestad exclusiva para modificarlo. La coherencia entre las copias se logra mediante un mecanismo de consenso, y la resistencia práctica a la alteración de los registros históricos se sustenta

mediante el encadenamiento criptográfico de bloques que se desarrollará en el apartado 2.2.

2.1.1 Elementos constitutivos

- **Nodo:** Equipo informático que participa en la red, almacena una copia total o parcial del libro mayor y, según su rol, valida, transmite o solo consulta transacciones.
- **Transacción:** Instrucción firmada digitalmente que modifica el estado del sistema (por ejemplo, la transferencia de un criptoactivo de una dirección a otra).
- **Dirección (*address*):** Identificador alfanumérico derivado de una clave pública, análogo funcional de una cuenta contable, pero sin vínculo intrínseco con la identidad de su titular.
- **Libro mayor distribuido (*ledger*):** Historial completo y ordenado cronológicamente de todas las transacciones válidas desde el bloque génesis.
- **Mecanismo de consenso:** Protocolo mediante el cual los nodos acuerdan qué versión del *ledger* es la válida (véase apartado 2.8).

Relevancia para la doctrina de contabilidad forense

Siguiendo la línea doctrinal desarrollada por Larry Crumbley en materia de contabilidad y litigios forenses, el perito debe distinguir con rigor entre el dato contable declarado por la entidad auditada (los estados financieros, los libros auxiliares, las conciliaciones) y el dato verificable de forma independiente en el propio protocolo blockchain. Esta dualidad de fuentes la declarada y la verificable es la piedra angular de la auditoría forense de criptoactivos, pues permite contrastar la narrativa contable de la administración con un registro externo que, cumplidas ciertas condiciones técnicas, resulta más difícil de manipular que una base de datos interna convencional.

Desde la óptica del gobierno corporativo y el control interno que promueve el *International Professional Practices Framework* (IPPF) del IIA marco cuyos componentes obligatorios fueron sustituidos, a partir de 2025, por las *Global Internal Audit Standards* del propio IIA la incorporación de blockchain en los procesos del negocio no elimina la necesidad de un sistema de control interno robusto; simplemente desplaza parte del riesgo desde la integridad del dato (que la tecnología puede reforzar) hacia la gobernanza de las claves criptográficas, la gestión de accesos y la calidad de los controles en la interfaz entre

el mundo *"off-chain"* (los sistemas contables y operativos tradicionales) y el mundo *"on-chain"* (el registro distribuido).

2.2 Estructura de bloques y cadenas

El bloque es la unidad elemental de almacenamiento en una blockchain. Cada bloque agrupa un conjunto de transacciones validadas durante un intervalo de tiempo determinado y se compone, típicamente, de un encabezado (*header*) y un cuerpo (*body*).

2.2.1 Componentes del encabezado del bloque

- **Hash del bloque anterior:** Enlace criptográfico que ancla el bloque actual al bloque precedente, generando el efecto de "cadena".
- **Marca de tiempo (*timestamp*):** Estimación del momento de creación del bloque, generada por el nodo o validador proponente y sujeta a los márgenes de tolerancia definidos por el protocolo; es relevante para establecer secuencia temporal en la reconstrucción pericial de hechos, pero no equivale, por sí sola, a una certificación legal de fecha u hora.
- **Raíz de Merkle (*Merkle root*):** Resumen criptográfico único que representa el conjunto de todas las transacciones incluidas en el bloque.
- **Nonce y datos de dificultad:** Valores empleados en redes con consenso por prueba de trabajo (*Proof of Work*) para validar el bloque (véase 2.8).
- **Número de bloque (*block height*):** Posición secuencial del bloque dentro de la cadena.

2.2.2 El árbol de Merkle como herramienta de auditoría

El árbol de Merkle merece atención especial porque ofrece al perito una herramienta de verificación selectiva de enorme valor práctico: permite demostrar que una transacción específica está incluida en un bloque determinado sin necesidad de descargar y validar la totalidad de las transacciones de ese bloque, mediante una prueba de inclusión (*Merkle proof*). Esta propiedad es explotable en procedimientos de auditoría de tipo confirmación externa, análo-

ga a la circularización de saldos bancarios, pero fundamentada en criptografía verificable en lugar de en la respuesta de un tercero.

2.2.3 Efecto de encadenamiento y resistencia práctica a la alteración

Cada bloque contiene el resultado de aplicar la función hash al bloque inmediatamente anterior. En consecuencia, alterar el contenido de un bloque histórico modificaría su hash, rompería el enlace con el bloque siguiente y, en cascada, con todos los bloques posteriores.

En redes con suficiente descentralización y poder de cómputo o de participación distribuido, rehacer esa cadena de forma coherente con la mayoría de los nodos resulta computacionalmente inviable en la práctica. Esta propiedad conocida como inmutabilidad práctica, y no absoluta es lo que otorga a la blockchain su valor como evidencia digital: no es que el dato sea imposible de alterar en términos matemáticos, sino que alterarlo de forma no detectable exige recursos que, en redes maduras y suficientemente descentralizadas, exceden ampliamente los de un atacante racional. Esta condición de seguridad está, por tanto, condicionada al diseño concreto del protocolo y a su mecanismo de consenso, y no debe generalizarse sin verificar el nivel de descentralización de la red específica examinada.

2.3 Hash criptográfico

La función hash criptográfica es el instrumento matemático que sostiene la integridad de toda la estructura descrita en el apartado anterior. Se trata de un algoritmo determinista que transforma una entrada de longitud arbitraria (un documento, una transacción, un bloque completo) en una salida de longitud fija, denominada resumen o huella digital (*digest*).

2.3.1 Propiedades exigibles a una función hash criptográfica

- **Determinismo:** La misma entrada produce siempre la misma salida.
- **Efecto avalancha:** Una variación mínima en la entrada (incluso un solo bit) produce una salida completamente distinta e impredecible.
- **Resistencia a preimagen:** Dado un resumen, resulta computacionalmente inviable reconstruir la entrada original.

- **Resistencia a colisiones:** Resulta computacionalmente inviable encontrar dos entradas distintas que produzcan el mismo resumen.
- **Eficiencia computacional:** El cálculo del resumen debe ser rápido, aunque su reversión debe ser prácticamente imposible.

2.3.2 Aplicaciones periciales del hash

Para el perito contable forense, el hash criptográfico es una herramienta transversal que excede el ámbito de los criptoactivos. Permite, entre otros usos:

Verificar la integridad de un archivo digital (por ejemplo, un respaldo de base de datos o un conjunto de comprobantes escaneados) calculando su resumen en el momento de la recolección de evidencia y comparándolo en etapas posteriores de la cadena de custodia.

Vincular criptográficamente la evidencia digital recolectada con un acta pericial, práctica que replica en el entorno digital el principio de cadena de custodia recogido en la metodología de investigación de fraude de la ACFE para la preservación de evidencia física y electrónica.

Identificar transacciones específicas en el explorador de bloques (*block explorer*) mediante su identificador único (TXID), que es en sí mismo un resumen hash de los datos de la transacción.

Detectar manipulación de documentación digital comparando el resumen de un documento cuestionado contra el resumen registrado en un sistema de sellado de tiempo (*timestamping*) previo, técnica cada vez más utilizada para anclar documentos corporativos a una blockchain pública como indicio de existencia en una fecha determinada (*proof of existence*), sin que ello equivalga automáticamente a una certificación notarial o legalmente vinculante de fecha; su fuerza probatoria dependerá del marco jurídico aplicable y de la evidencia complementaria disponible.

2.4 Redes públicas, privadas e híbridas

La clasificación de las redes blockchain según su modelo de gobernanza y de control de acceso resulta determinante para el diseño del programa de auditoría, pues condiciona tanto la disponibilidad de evidencia externa verificable como el perfil de riesgo AML/CFT asociado.

2.4.1 Redes públicas o sin permiso (*permissionless*)

En principio, cualquier persona puede ejecutar un nodo y consultar el historial de transacciones sin autorización previa de una autoridad central; sin embargo, la posibilidad efectiva de participar en el proceso de validación depende de las reglas del protocolo (por ejemplo, capacidad de cómputo disponible en redes de prueba de trabajo o volumen de criptoactivo en garantía en redes de prueba de participación). Tampoco todos los nodos almacenan necesariamente el historial completo: coexisten nodos completos, nodos ligeros y nodos de archivo con distintos alcances de almacenamiento y verificación. Ejemplos representativos son Bitcoin y Ethereum.

Su principal ventaja pericial es la transparencia: el historial completo es públicamente auditable a través de exploradores de bloques y herramientas de análisis *on-chain*. Su principal riesgo, desde la perspectiva de las metodologías de análisis de riesgo AML/CFT, es el seudonimato de las direcciones, que exige técnicas de análisis de clústeres y de atribución de titularidad (véase el capítulo del presente manual dedicado a trazabilidad blockchain).

2.4.2 Redes privadas o con permiso (*permissioned*)

El acceso a la red, la operación de nodos y, en muchos casos, la consulta del *ledger* están restringidos a un conjunto cerrado de participantes autorizados por una entidad gestora o un consorcio. Son frecuentes en aplicaciones bancarias, cadenas de suministro y proyectos interbancarios. Desde el punto de vista del control interno bajo el marco COSO y los marcos de referencia del IIA, estas redes concentran el riesgo de gobernanza en el administrador de la red y en la política de asignación de permisos, por lo que el auditor debe examinar con especial rigor la matriz de roles y privilegios de los nodos validadores y administradores.

2.4.3 Redes híbridas y de consorcio

Combinan elementos de ambos modelos: pueden mantener capas públicas de anclaje (*anchoring*) sobre una blockchain pública para dotar de mayor integridad verificable a un registro que, en su operación cotidiana, funciona en un entorno permisionado. Es el modelo que con mayor frecuencia adoptan las iniciativas de tokenización de activos financieros impulsadas por bancos y asociaciones bancarias iberoamericanas, que buscan conciliar la eficiencia

operativa de una red controlada con la resistencia práctica a la manipulación propia de una red pública.

Tabla No. 7

Matriz comparativa: Modelos de red blockchain y perfil de riesgo pericial

Modelo de red	Grado de transparencia	Control de gobernanza	Riesgo AML/CFT típico
Pública (*permissionless*)	**Alto:** *Ledger* abierto y auditable por cualquier analista mediante exploradores de bloques.	**Difuso:** Gobernado por esquemas de consenso distribuido global sin un administrador central.	Seudonimato de transacciones, uso de mezcladores (*mixers*), saltos entre cadenas y *exchanges* no regulados.
Privada (*permissioned*)	**Restringido:** Limitado exclusivamente a los participantes autorizados por la red.	**Concentrado:** Radicado en el administrador de la red o entidad gestora del consorcio.	Colusión interna, manipulación de permisos de acceso, y procesos de debida diligencia (KYC) insuficientes por parte del operador.
Híbrida / consorcio	**Variable:** Depende de la capa consultada (pública de anclaje vs. privada operativa).	**Compartido:** Distribuido de manera concertada entre los miembros del consorcio.	Desafíos de interoperabilidad entre capas y riesgos de arbitraje regulatorio entre distintas jurisdicciones.

2.5 Contratos inteligentes (*Smart contracts*)

Los contratos inteligentes (*smart contracts*) son programas informáticos almacenados en una infraestructura blockchain que codifican reglas de negocio y ejecutan la lógica programada cuando son invocados mediante una transacción u otro evento reconocido por el protocolo, sin intervención discrecional de un intermediario en el momento de la ejecución. No se trata, en consecuencia, de una ejecución espontánea, sino condicionada a la invocación del contrato y a las reglas de validación de la red.

2.5.1 Naturaleza jurídico-contable

Para efectos de auditoría y peritaje, el *smart contract* debe analizarse en una doble dimensión:

- Como **código fuente auditable**, expuesto a vulnerabilidades y errores de programación que pueden ser objeto de explotación fraudulenta.
- Como **generador automático de hechos económicos** con efectos contables directos, en la medida en que su ejecución puede originar transferencias de criptoactivos, emisión de tokens, distribución de rendimientos o liquidación de garantías.

2.5.2 Riesgos de control interno y de fraude

- **Riesgo de código:** Errores de programación (*bugs*), condiciones de reentrada (*reentrancy*) o lógica mal diseñada que permiten la sustracción o el bloqueo indebido de fondos.
- **Riesgo de gobernanza del contrato:** Existencia de funciones administrativas privilegiadas ("funciones de puerta trasera" o *backdoors*) que permiten a un desarrollador o a una clave privilegiada modificar parámetros, pausar operaciones o retirar fondos, lo cual erosiona la premisa de descentralización y constituye un punto de concentración de riesgo análogo a una segregación de funciones deficiente en un ERP tradicional.
- **Riesgo de oráculo:** Dependencia de fuentes externas de datos (*oracles*) para alimentar de información al contrato; su manipulación puede inducir ejecuciones fraudulentas (por ejemplo, mediante ataques de manipulación de precios en protocolos de finanzas descentralizadas).
- **Riesgo de auditoría de código insuficiente:** Despliegue de contratos sin revisión independiente por firmas especializadas en auditoría de código o sin pruebas formales de verificación (*formal verification*).

Aplicando el marco conceptual del triángulo del fraude, desarrollado en la metodología de investigación de fraude de la ACFE, el perito debe identificar en los contratos inteligentes tanto la oportunidad (vulnerabilidades técnicas o funciones administrativas no divulgadas) como los mecanismos de racionalización y ocultamiento propios de esquemas de apropiación de activos digitales, adaptando los procedimientos clásicos de indagación de fraude ocupacional al examen de código fuente y de eventos emitidos por el contrato (*logs on-chain*).

2.5.3 Procedimientos periciales sugeridos

Obtención y verificación del código fuente publicado frente al *bytecode* efectivamente desplegado en la red (verificación de contrato).

Identificación de direcciones con privilegios administrativos (*owner, admin, multisig*) y su titularidad.

Revisión de auditorías de seguridad previas realizadas por terceros especializados y de su alcance declarado.

Reconstrucción de la secuencia de eventos (*event logs*) emitidos por el contrato para trazar flujos de valor relevantes para el caso investigado.

2.6 Exchanges centralizados y descentralizados

Los exchanges de criptoactivos constituyen la principal interfaz de conversión entre moneda fiduciaria y criptoactivos, por lo que concentran una parte sustancial del riesgo AML/CFT del ecosistema. Su clasificación en centralizados y descentralizados determina de forma directa la disponibilidad de evidencia, el eventual sujeto obligado frente al régimen de prevención de lavado de activos y la metodología de obtención de información en el marco de una investigación forense.

2.6.1 Exchanges centralizados (CEX)

Operan como intermediarios que custodian los criptoactivos de sus usuarios, mantienen un libro de órdenes interno (*order book*) y, en la medida en que sean regulados como Proveedores de Servicios de Activos Virtuales (VASP) conforme a las Recomendaciones del GAFI cuya implementación efectiva depende de la trasposición normativa de cada jurisdicción, quedan sujetos a obligaciones de debida diligencia del cliente, monitoreo de transacciones y reporte de operaciones sospechosas.

Para el auditor, los CEX ofrecen una ventaja probatoria relevante cuando dichos controles existen: mantienen registros internos (*off-chain*) de identidad del cliente, historial de órdenes y direcciones de depósito y retiro, susceptibles de ser requeridos mediante los mecanismos de cooperación judicial o de solicitud directa que resulten aplicables.

2.6.2 Exchanges descentralizados (DEX)

Operan mediante contratos inteligentes que ejecutan intercambios de forma automática (frecuentemente bajo el modelo de creadores de mercado automatizados o AMM), sin custodia centralizada de los fondos del usuario y, en la capa del protocolo, habitualmente sin un proceso estricto de identificación del cliente (KYC). Ello no implica, sin embargo, ausencia total de sujetos obligados: las interfaces web, los operadores del *front-end*, los proveedores de liquidez institucionales u otros participantes pueden estar sujetos a obligaciones de debida diligencia según el marco regulatorio de cada jurisdicción.

Esta configuración seudonimato predominante a nivel de protocolo, con obligaciones eventualmente dispersas en la capa de interfaz u operación convierte a los DEX en un punto de atención prioritario en las matrices de riesgo AML/CFT, particularmente en tipologías de *layering* (recolección y estratificación) dentro del ciclo de lavado de activos, dado que permiten intercambiar activos digitales de forma prácticamente instantánea y con escasa fricción de cumplimiento en la capa de protocolo.

2.6.3 Modelos híbridos y agregadores

Existen plataformas híbridas que combinan liquidez centralizada y descentralizada, así como agregadores que enrutan órdenes entre múltiples DEX para optimizar el precio y reducir el deslizamiento (*slippage*). Estos modelos incrementan la complejidad del rastreo pericial, pues una sola operación de intercambio iniciada por el usuario puede fragmentarse en múltiples transacciones *on-chain* ejecutadas a través de distintos protocolos subyacentes.

2.7 Wallets y sistemas de custodia

Matriz comparativa: CEX vs. DEX y consideraciones periciales

Factor de riesgo	Exchange centralizado (CEX)	Exchange descentralizado (DEX)	Consideración pericial
Debida diligencia del cliente	Generalmente exigida cuando existe regulación aplicable (KYC / EDD).	Habitualmente inexistente a nivel de protocolo; puede existir en la interfaz u operador, según la jurisdicción.	Verificar si el VASP o el operador de la interfaz web se encuentra debidamente registrado o supervisado.

Disponibilidad de evidencia de identidad	**Alta**, sujeta a los canales de cooperación y requerimiento legal al intermediario.	**Nula** a nivel de protocolo; se dispone únicamente de una dirección seudónima.	Complementar el análisis técnico con herramientas de análisis de clústeres e inteligencia de fuentes abiertas (OSINT).
Trazabilidad de fondos	Registros contables internos (*off-chain*) cruzados con el registro en la blockchain (*on-chain*).	Únicamente registros distribuidos en la blockchain, salvo trazas propias del operador de la interfaz.	El explorador de bloques constituye una fuente primaria indispensable, pero no la única en la reconstrucción del caso.
Punto de control regulatorio	El propio exchange actúa como sujeto obligado potencial frente al régimen de prevención.	El código del protocolo carece de un sujeto obligado tradicional; puede recaer de forma difusa en la interfaz.	Evaluar la exposición transaccional a sanciones internacionales (como listas OFAC) y restrictivas.

2.8 Wallets o monederos digitales

La wallet o monedero digital no almacena, en sentido estricto, criptoactivos; almacena y gestiona las claves criptográficas principalmente la clave privada que otorgan control sobre los activos registrados en la blockchain a nombre de una dirección determinada. La comprensión precisa de esta distinción es indispensable para el auditor, pues el objeto real de custodia, control interno y riesgo de fraude no es el token en sí, sino la clave privada que habilita su transferencia.

2.8.1 Clasificación según conectividad

- **Wallets calientes (*hot wallets*):** Mantienen las claves privadas en dispositivos conectados a internet, lo que facilita la operatividad transaccional pero incrementa la superficie de exposición a ataques informáticos remotos.
- **Wallets frías (*cold wallets*):** Almacenan las claves privadas en dispositivos o soportes sin conexión permanente a internet (como carteras de hardware o almacenamiento *air-gapped*), reduciendo drásticamente el riesgo de sustracción remota a cambio de una menor agilidad operativa.

2.8.2 Clasificación según el modelo de custodia

- **Custodia propia (*self-custody / non-custodial*):** El titular controla directamente su clave privada, sin intermediarios. Ofrece autonomía plena, pero traslada íntegramente al usuario el riesgo de pérdida de la clave o de la frase semilla (*seed phrase*), sin posibilidad de recuperación por un tercero.
- **Custodia por terceros (*custodial*):** Una entidad típicamente un exchange centralizado o un custodio institucional regulado controla las claves privadas en representación del cliente. Este modelo concentra el riesgo en la solvencia, los controles internos y la ciberseguridad del custodio, y es el que con mayor naturalidad se integra en un programa de auditoría financiera tradicional, al permitir procedimientos de confirmación externa con el tercero custodio.
- **Custodia mediante firma múltiple (*multisignature* o *multisig*):** Requiere la autorización concurrente de varias claves privadas, controladas por distintas personas o dispositivos, para autorizar una transacción. Constituye una de las herramientas de control interno más eficaces frente al riesgo de fraude por concentración de autoridad, al replicar en el entorno criptográfico el principio de doble o múltiple autorización.

2.8.3 Implicaciones para el control interno y la evidencia forense

Bajo el enfoque de control interno que promueven los marcos de referencia del IIA (el IPPF histórico y las vigentes *Global Internal Audit Standards*), la gestión de claves privadas debe evaluarse como un proceso crítico equivalente a la custodia de efectivo, títulos valores o llaves de bóveda. Exige segregación de funciones entre quien genera las claves, quien las custodia y quien autoriza su uso operativo, así como procedimientos documentados de generación, respaldo (*backup*), recuperación ante contingencias y revocación inmediata en caso de desvinculación de personal.

2.9 Minería y validación de transacciones

La minería y, más ampliamente, la validación de transacciones son los procesos mediante los cuales una red blockchain determina qué transacciones se incorporan a un nuevo bloque y logra que la mayoría de los nodos converjan

en una única versión válida del *ledger*. El mecanismo de consenso empleado condiciona directamente la seguridad, la velocidad, el consumo energético y lo que interesa particularmente al perito la solidez de la resistencia práctica a la alteración descrita en el apartado 2.2.

2.9.1 Prueba de trabajo (*Proof of Work, PoW*)

Los nodos denominados mineros compiten por resolver un problema criptográfico computacionalmente costoso; el primero en resolverlo obtiene el derecho a proponer el siguiente bloque y recibe una recompensa en criptoactivo nativo de la red. La seguridad del sistema descansa en que reescribir el histórico exigiría superar el poder de cómputo agregado (*hash rate*) de la mayoría honesta de la red, lo que resulta económicamente inviable en redes de gran escala como Bitcoin, pero constituye un riesgo real y documentado en redes de menor capitalización, expuestas a los llamados ataques del 51 %.

2.9.2 Prueba de participación (*Proof of Stake, PoS*) y variantes

Los validadores son seleccionados para proponer y confirmar bloques en función de la cantidad de criptoactivo que han bloqueado como garantía (*staking*), en lugar de su poder de cómputo. El incentivo económico se invierte respecto de la PoW: el validador cuya conducta resulte protocolariamente verificable como deshonesta o contradictoria por ejemplo, firmar simultáneamente bloques o mensajes de consenso incompatibles (*equivocation*) puede perder parte de su garantía bloqueada mediante sanciones de *slashing*; la inactividad o desconexión del validador, en cambio, suele dar lugar a penalizaciones distintas y generalmente de menor severidad (por ejemplo, mecanismos de *inactivity leak* o reducción de recompensas), según las reglas específicas de cada protocolo. Ethereum migró a este modelo, y es también el mecanismo predominante en numerosas redes de nueva generación y en plataformas orientadas a la tokenización institucional.

2.9.3 Otros mecanismos relevantes

- **Prueba de autoridad (*Proof of Authority*):** Un conjunto reducido y preidentificado de validadores autorizados confirma los bloques; es propio

de redes privadas o de consorcio donde la identidad de los validadores es conocida y contractualmente responsable.

- **Tolerancia a fallas bizantinas prácticas (PBFT) y variantes:** Empleadas en redes permisionadas orientadas a una alta velocidad de finalización transaccional, frecuentes en proyectos de infraestructura DLT impulsados por consorcios bancarios.

2.9.4 Confirmaciones y finalidad transaccional

El número de confirmaciones esto es, la cantidad de bloques añadidos con posterioridad al bloque que contiene una transacción determinada es un indicador técnico directamente relevante para la opinión pericial sobre la firmeza de una transacción. A mayor número de confirmaciones, menor la probabilidad estadística de que dicha transacción sea revertida mediante una reorganización de cadena (*chain reorg*).

En la práctica de la industria es habitual que cada organización defina, como política interna de gestión de riesgo, un umbral de confirmaciones diferenciado según el activo, la red, el valor económico de la operación, el grado de descentralización y su propia tolerancia al riesgo. Dicho umbral, cuando exista, debe documentarse expresamente y motivarse caso por caso al momento de certificar la evidencia *on-chain* incorporada al informe pericial, sin atribuirse a un estándar sectorial general salvo que pueda identificarse una fuente concreta y verificable.

3 ECOSISTEMA FINANCIERO DIGITAL Y NUEVOS MODELOS DE NEGOCIO

3.1 Fundamentos generales de los criptoactivos y la tecnología blockchain

Los criptoactivos constituyen representaciones digitales de valor o derechos que pueden ser transferidos y almacenados electrónicamente mediante tecnologías de registro distribuido *Distributed Ledger Technology* (DLT) u otras tecnologías similares. Su desarrollo acelerado ha generado nuevas formas de intercambio, inversión, financiamiento, prestación de servicios financieros y organización empresarial.

El concepto es significativamente más amplio que el de la tradicional criptomoneda. Dentro del ecosistema actual pueden encontrarse:

- Criptoactivos de pago.
- Monedas estables (*stablecoins*).
- Tokens de utilidad (*utility tokens*).
- Tokens vinculados a activos (*asset-referenced tokens*).
- Tokens no fungibles (NFT).
- Activos tokenizados y otros instrumentos digitales.

El Consejo de Estabilidad Financiera (FSB) considera que los criptoactivos comprenden distintos segmentos interrelacionados, entre ellos los criptoactivos no respaldados, las *stablecoins* y las finanzas descentralizadas (DeFi), por lo que deben analizarse como un ecosistema integral y sistémico.

Desde una perspectiva económica, la tecnología blockchain permite modificar profundamente el modelo tradicional de intermediación. Mientras que el sistema financiero convencional utiliza instituciones centrales como bancos, bolsas de valores, cámaras de compensación y custodios, las redes blockchain pueden utilizar criptografía, consenso distribuido y contratos inteligentes para registrar y ejecutar determinadas operaciones de forma automatizada.

En concordancia, el Banco de Pagos Internacionales (BIS**)** señala que el ecosistema cripto comprende diferentes capas interconectadas:

1. Infraestructura DLT.
2. Entidades financieras centralizadas y descentralizadas.

3. Organizaciones autónomas descentralizadas (DAOs).
4. Billeteras digitales.
5. Relaciones *peer-to-peer* (de igual a igual).

Tabla No. 6

Elementos fundamentales del ecosistema financiero digital

Elemento	Fundamento
Blockchain	Registro distribuido e inmutable de transacciones.
Criptoactivo	Representación digital de valor o derechos susceptibles de transferencia y almacenamiento electrónico.
Token	Unidad digital que representa un valor, derecho, utilidad o activo específico dentro de una red.
Smart contract	Código autoejecutable que permite validar y ejecutar condiciones previamente programadas sin intermediarios.
Wallet	Medio tecnológico para gestionar claves criptográficas y administrar activos digitales.
Exchange	Plataforma centralizada o descentralizada para el intercambio de activos digitales.
DeFi (Finanzas descentralizadas)	Servicios financieros prestados mediante protocolos abiertos y contratos inteligentes.
DAO (Organización autónoma descentralizada)	Estructura organizativa gobernada mediante reglas codificadas y mecanismos de votación digital.
Tokenización	Proceso de conversión y representación digital de activos o derechos físicos/financieros mediante tokens.
P2P (*Peer-to-Peer*)	Transferencia directa e interactiva de valor o información entre participantes, sin intermediarios institucionales.
Web3	Nuevo modelo de Internet fundamentado en la descentralización, la propiedad digital de los usuarios y los protocolos blockchain.

La **Organización para la Cooperación y el Desarrollo Económicos (OCDE)** considera que la tokenización puede representar activos físicos o financieros en registros distribuidos o generar tokens nativos de blockchain, identificándola como una de las aplicaciones más relevantes de la tecnología DLT en los mercados financieros contemporáneos.

3.2 Finanzas descentralizadas (DeFi)

Las Finanzas Descentralizadas (*Decentralized Finance*, DeFi) constituyen un conjunto de aplicaciones y protocolos financieros construidos principalmente sobre redes blockchain, cuyo propósito es proporcionar las funciones tradicionalmente ejecutadas por los intermediarios financieros.

Entre sus principales actividades operativas se encuentran:

- Préstamos y créditos.
- Intercambio de activos.
- Provisión de liquidez y generación de rendimientos mediante protocolos.
- Inversión y derivados financieros.
- Gestión de activos y pagos.

El **Banco de Pagos Internacionales (BIS)** señala que DeFi busca reproducir las funciones de las finanzas tradicionales mediante protocolos abiertos, blockchain y contratos inteligentes, sustituyendo de forma progresiva la intermediación institucional tradicional por código autoejecutable.

3.2.1 Modelo de funcionamiento

El flujo operativo general de un protocolo DeFi se articula de la siguiente manera:



- **Ejemplo práctico:** Un usuario deposita un criptoactivo en un protocolo el contrato inteligente registra formalmente el depósito otro usuario obtiene un préstamo en condiciones automatizadas las reglas del préstamo se ejecutan sin intervención humana los intereses generados

se distribuyen automáticamente según los parámetros predefinidos del protocolo.

3.2.2 Nuevos modelos de negocio en DeFi

El ecosistema descentralizado permite desarrollar modelos operativos innovadores, tales como:

- Plataformas descentralizadas de préstamos y créditos (*lending*).
- Exchanges descentralizados (DEX).
- Plataformas de participación y rendimiento (*staking*).
- Protocolos de provisión de liquidez (*liquidity pools*).
- Mercados de derivados descentralizados.
- Administración automatizada de carteras y activos.
- Servicios financieros descentralizados de alta velocidad.

3.2.3 Riesgos y consideraciones para la auditoría forense

Para una investigación de auditoría forense o evaluación de control interno, adquieren particular relevancia los siguientes riesgos sistémicos y operativos:

- Vulnerabilidades y fallas lógicas en los contratos inteligentes.
- Manipulación de precios (ataques de manipulación de oráculos o arbitraje malicioso).
- Ataques informáticos e intrusiones a protocolos.
- Pérdida o compromiso de claves privadas.
- Concentración indebida de gobernanza y control de protocolos.
- Fraude y esquemas de malversación digital.
- Riesgos de lavado de activos y financiamiento ilícito a través de operaciones sin identificación suficiente (*unhosted wallets*).
- Riesgos críticos de liquidez y apalancamiento excesivo.
- Dependencia crítica de oráculos externos para la alimentación de datos.

En concordancia, el Consejo de Estabilidad Financiera (FSB) y el BIS advierten que el ecosistema DeFi puede presentar vulnerabilidades sistémicas severas relacionadas con crisis de liquidez, apalancamiento desmedido, alta interconexión entre protocolos y fragilidades operativas intrínsecas.

3.3 Monedas digitales de bancos centrales (CBDC)

Las Monedas Digitales de Bancos Centrales (*Central Bank Digital Currencies*, CBDC) son formas digitales de dinero fiduciario emitidas de manera directa y respaldadas por un banco central.

Es fundamental diferenciarlas conceptualmente de las criptomonedas privadas y los criptoactivos no respaldados. Sobre esta materia, el BIS ha establecido como principios fundamentales que una CBDC debe:

Coexistir de manera armónica con el dinero en efectivo y el dinero bancario tradicional.

Contribuir a mantener la estabilidad monetaria y financiera general.

Garantizar la confianza pública en el sistema de pagos y en la moneda nacional.

Tabla No. 7

Comparativa entre CBDC y Criptoactivos Privados

Dimensión / Criterio	CBDC (Moneda Digital de Banco Central)	Criptoactivo Privado
Entidad Emisora	Emitida directamente por un banco central.	Generalmente emitido por una entidad privada, fundación o protocolo descentralizado.
Naturaleza del Valor	Representa dinero soberano de curso legal.	Representa valor privado o derechos específicos sobre un ecosistema.
Arquitectura de Control	Centralización institucional (bajo la gobernanza del banco central).	Puede utilizar esquemas de descentralización o gobernanza distribuida.
Política Monetaria	Instrumento directo de transmisión y ejecución de política monetaria.	No está vinculada a los objetivos de la política monetaria oficial.
Marco Jurídico	Sustentado en un marco jurídico público y regulatorio estricto.	Su marco jurídico y regulatorio varía según cada jurisdicción.
Objetivo Principal	Estabilidad monetaria, eficiencia en pagos y seguridad financiera.	Fines diversos de pago, inversión, especulación, utilidad o gobernanza.

3.3.1 Modalidades de CBDC

Las Monedas Digitales de Bancos Centrales se estructuran fundamentalmente en dos grandes modalidades según su segmento de aplicación:

- **CBDC minorista (*retail*):** Destinada al público general (personas naturales y empresas), orientada a facilitar pagos cotidianos, transferencias de bajo monto y operaciones de comercio electrónico.
- **CBDC mayorista (*wholesale*):** Utilizada exclusivamente entre instituciones financieras y el banco central para la liquidación interbancaria de valores, pagos de alto valor y operaciones transfronterizas.

3.3.2 Potencial para nuevos modelos de negocio

El desarrollo de las CBDC abre la puerta a arquitecturas financieras innovadoras que permiten:

- Pagos programables condicionales.
- Optimización de pagos transfronterizos.
- Liquidación instantánea de valores tokenizados (*Delivery versus Payment* - DvP).
- Ejecución de contratos financieros automatizados.
- Reducción estructural de costos de intermediación.
- Mayor inclusión financiera respaldada por moneda soberana.

El Banco de Pagos Internacionales (BIS**)** destaca precisamente la posibilidad de combinar dinero digital de banco central, tokenización y programabilidad para construir una nueva infraestructura monetaria y financiera global.

Nota crítica: Una CBDC no debe confundirse conceptual ni jurídicamente con un criptoactivo privado. Son categorías regulatorias y económicas completamente diferenciadas.

3.4 DAOs y gobernanza descentralizada

Una DAO (*Decentralized Autonomous Organization* u Organización Autónoma Descentralizada) es una estructura organizativa que utiliza tecnología blockchain, contratos inteligentes y mecanismos de votación basados en tokens para coordinar las decisiones colectivas de una comunidad sin necesidad de una jerarquía gerencial tradicional.

En términos simplificados, su ciclo operativo responde al siguiente flujo:

Reglas Smart ContractTokens de GobernanzaVotaciónEjecución en Blockchain

Las decisiones comunitarias pueden comprender:

- Modificación de parámetros o lógicas de protocolos.
- Utilización, asignación y desembolso de fondos comunitarios del tesoro.
- Incorporación de nuevas funcionalidades o integraciones.

- Distribución de recursos e incentivos.
- Actualización de contratos inteligentes.

El BIS identifica a las DAOs como estructuras que operan sobre redes distribuidas, utilizando reglas codificadas inalterablemente en contratos inteligentes para su gobernanza.

3.4.1 Modelos de negocio en DAOs

Una DAO se apoya habitualmente en componentes como:

- Emisión y tenencia de tokens de gobernanza.
- Fondos comunitarios descentralizados (*Treasuries*).
- Sistemas automatizados de votación ponderada.
- Integración directa con plataformas DeFi.
- Administración colectiva de proyectos de desarrollo e innovación.
- Mecanismos de financiación descentralizada (*crowdfunding* basado en blockchain).

3.4.2 Problemática jurídica y enfoque forense

En este punto emerge un aspecto crítico para la auditoría forense y la investigación legal: la descentralización tecnológica no implica en absoluto ausencia de responsabilidad jurídica.

El BIS advierte que muchas estructuras autodenominadas DAOs mantienen en la práctica grados muy elevados de centralización fáctica, operando a través de la concentración de propiedad de tokens, bloques de votación mayoritarios o el control exclusivo de llaves administrativas privilegiadas (*multisig keys*).

Por consiguiente, en cualquier peritaje forense o investigación de una DAO debe indagarse rigurosamente:

1. ¿Quién creó y desplegó los contratos iniciales?
2. ¿Quién controla realmente los mecanismos de votación o el tesoro?
3. ¿Quién posee el poder de voto efectivo (*whales* o ballenas de gobernanza)?
4. ¿Quién administra las llaves criptográficas con privilegios de emergencia o actualización?
5. ¿Quién recibe en última instancia los beneficios económicos?
6. ¿Quién ejecuta materialmente las decisiones?

3.5 Web3

La Web3 representa una evolución conceptual de Internet hacia un modelo en el cual la tecnología blockchain permite incorporar dimensiones económicas y de soberanía digital que las versiones anteriores no poseían.

La distinción conceptual de las eras de Internet puede expresarse operativamente de la siguiente forma:

- **Web1:** Leer (contenido estático y unidireccional).
- **Web2:** Leer + Interactuar (plataformas centralizadas, redes sociales y bidireccionalidad).
- **Web3:** Leer + Interactuar + Poseer / Intercambiar activos digitales (descentralización, propiedad nativa y valor soberano).

Blockchain proporciona aquí la infraestructura inalterable para registrar propiedad, derechos, transacciones y participación económica directa.

3.5.1 Nuevos modelos de negocio en Web3

- Plataformas y aplicaciones descentralizadas (DApps).
- Mercados digitales (*marketplaces* nativos).
- Ecosistemas de juegos basados en blockchain (*GameFi*).
- Nuevas economías virtuales e incentivos por participación.
- Creación y monetización de comunidades digitales.
- Tokens de utilidad y gobernanza.
- Activos no fungibles (NFT).
- Servicios financieros descentralizados (DeFi) e identidad digital soberana.

No obstante, Web3 no constituye por sí misma una categoría jurídica autónoma. Las actividades económicas desarrolladas mediante Web3 quedan plenamente sometidas a la normativa sectorial aplicable según su función económica real, en estricta concordancia con el principio regulatorio del Consejo de Estabilidad Financiera (FSB) de “misma actividad, mismo riesgo, misma regulación”.

3.6 NFT y tokenización de activos

Los Non-Fungible Tokens (NFT) son criptoactivos diseñados para representar unidades digitales diferenciadas, únicas e indivisibles dentro de una red DLT.

A diferencia de un token fungible (donde rige la equivalencia perfecta, ej.), un NFT posee metadatos y atributos exclusivos que determinan que:

$$NFT_A \neq NFT_B$$

Pueden utilizarse para representar una gran diversidad de elementos:

- Arte digital y coleccionables multimedia.
- Entradas y tiques de acceso a eventos.
- Certificados académicos y credenciales profesionales.
- Derechos de acceso y membresías exclusivas.
- Activos, avatares y elementos dentro de videojuegos.
- Identidad digital verificable y derechos específicos sobre bienes.

El Grupo de Acción Financiera Internacional (FATF / GAFI) advierte que la clasificación regulatoria de un NFT depende estrictamente de su naturaleza y uso económico efectivo, y no simplemente de la denominación tecnológica que se le atribuya. Si en la práctica se emplea como medio de pago o instrumento de inversión especulativa, quedará plenamente comprendido dentro de los estándares regulatorios aplicables a los activos virtuales.

3.6.1 Tokenización de activos

La tokenización consiste en representar digitalmente un activo físico, un derecho creditorio o un instrumento financiero mediante tokens registrados en una blockchain o DLT.

Ejemplos de conversión:

- Inmueble físico → Tokenización → Tokens digitales fraccionados de propiedad.
- Bono corporativo → Tokenización → Token financiero de deuda.
- Obra de arte → Tokenización → Token de copropiedad.
- Factura comercial → Tokenización → Representación digital negociable (*factoring* DLT).

La OCDE identifica a la tokenización como una innovación con alto potencial para transformar la eficiencia de los mercados financieros, aunque señala que persisten importantes obstáculos operativos, regulatorios y de interoperabilidad para su adopción masiva global.

3.6.2 Aplicaciones prácticas y riesgo forense

- Fraccionamiento de activos ilíquidos o de alto valor.
- Nuevos canales de financiación alternativa.
- Dinamización de mercados secundarios.
- Constitución de garantías digitales eficientes.
- Administración y custodia automatizada de activos.

Riesgo forense crítico: En el análisis legal y pericial, debe tenerse siempre presente que Un token puede constituir la representación técnica de un derecho, pero el perito debe verificar rigurosamente en el plano legal qué derecho real o contractual se está transmitiendo y si el marco jurídico de la jurisdicción reconoce dicha titularidad.

3.7 Stablecoins (Monedas estables)

Las *stablecoins* son criptoactivos diseñados específicamente para mantener un valor relativamente estable respecto de un activo de referencia, normalmente una moneda fiduciaria de curso legal como el dólar estadounidense (USD), aunque también pueden estar vinculadas a materias primas, cestas de activos u otros mecanismos algorítmicos.

Sus principales tipologías comprenden:

1. **Respaldadas por moneda fiduciaria o activos financieros tradicionales** (mantenidos en reservas físicas o bancarias).
2. **Respaldadas por sobrecolateralización en otros criptoactivos**.
3. **Algorítmicas** (reguladas mediante la contracción o expansión automatizada de su oferta monetaria por código).

El **BIS** explica que las stablecoins buscan mitigar la alta volatilidad característica de los criptoactivos tradicionales mediante mecanismos de respaldo y reservas, habiéndose consolidado como el principal medio de intercambio y pasarela de liquidez dentro del ecosistema cripto.

3.7.1 Funciones y riesgos asociados

- **Funciones principales:** Medio generalizado de intercambio, reserva temporal de valor frente a la volatilidad, puerta de entrada y salida (*on-ramp / off-ramp*) hacia los mercados cripto, pagos transfronterizos y provisión central de liquidez en protocolos DeFi.

- **Riesgos críticos:** Insuficiencia o mala calidad de las reservas de respaldo, riesgo de corrida o fallo en el rescate (*redemption risk*), opacidad en las auditorías de reservas, concentración de mercado, riesgo de contraparte, riesgo tecnológico de los contratos de emisión y vulnerabilidad frente a operaciones de lavado de activos.

El **Consejo de Estabilidad Financiera (FSB)** ha desarrollado recomendaciones regulatorias estrictas y específicas para las stablecoins de alcance global, debido al potencial riesgo sistémico que representan para la estabilidad financiera internacional.

3.8 Metaverso

El metaverso se entiende como un conjunto de entornos digitales inmersivos, interoperables y persistentes en los cuales los usuarios pueden interactuar, trabajar, comerciar, crear bienes digitales y desarrollar complejas actividades económicas.

La tecnología blockchain aporta a estos espacios virtuales elementos clave como:

- Propiedad digital soberana y verificable.
- Identificación inequívoca de activos mediante registros distribuidos.
- Integración nativa de NFT y tokens de utilidad.
- Sistemas de pagos interoperables y economías virtuales descentralizadas.
- Contratos inteligentes para la automatización de transacciones y gobernanza de tierras virtuales.

Flujo operativo típico:

UsuarioAvatar Metaverso Compra NFTTokenWalletBlockchain

3.8.1 Nuevos modelos de negocio en el metaverso

- Comercio y diseño de bienes virtuales (*digital wearables*).
- Adquisición y arrendamiento de inmuebles virtuales (*virtual real estate*).
- Producción y monetización de eventos digitales masivos.
- Publicidad inmersiva y experiencias de marca.
- Videojuegos interactivos con economías basadas en jugadores (*Play-to-Earn / Play-and-Own*).

- Prestación de servicios profesionales especializados dentro de entornos virtuales.

Precaución técnica y forense: El metaverso no equivale a blockchain. Blockchain es una tecnología subyacente que puede o no utilizarse dentro de un metaverso; de hecho, existen múltiples entornos virtuales centralizados que operan sin registros distribuidos.

Desde la **perspectiva forense**, el metaverso presenta desafíos complejos que exigen investigar:

1. La identificación jurídica fehaciente del propietario real tras un avatar.
2. La trazabilidad de transacciones en economías cerradas o interoperables.
3. La autenticidad y valoración pericial de activos virtuales.
4. La tipificación de conductas defraudatorias, apropiación indebida de bienes digitales y delitos informáticos cometidos en jurisdicciones múltiples.

3.9 Plataformas P2P (*Peer-to-Peer*)

Las plataformas *Peer-to-Peer* permiten que dos participantes intercambien valor, divisas o criptoactivos directamente entre sí, sin la intervención de un intermediario financiero tradicional centralizado.

Flujo operativo:

Persona WalletBlockchainWalletPersona B

Pueden emplearse para:

- Transferencias directas de criptoactivos.
- Compraventa de activos digitales (*fiat-to-crypto* mediante depósitos bancarios o pasarelas).
- Préstamos directos entre particulares.
- Pagos y remesas internacionales de bajo costo.

El **GAFI (FATF)** reconoce a las transacciones P2P como un área de altísimo riesgo dentro del lavado de activos y el financiamiento del terrorismo, enfatizando la necesidad imperativa de que los Estados comprendan, monitoreen y mitiguen los riesgos asociados a las transacciones no intermediadas y el uso de monederos no alojados (*unhosted wallets*).

3.9.1 Ventajas y riesgos operativos

- **Ventajas:** Supresión de intermediarios institucionales, disponibilidad operativa continua (24/7), alcance global transfronterizo, rapidez en la ejecución y reducción potencial de costos transaccionales.
- **Riesgos forenses:** Anonimato o pseudonimato reforzado, exposición a esquemas de fraude (*scams* y estafas de triangulación de pagos), ejecución de operaciones ilícitas, severa dificultad para la identificación de contrapartes, ausencia de mecanismos institucionales tradicionales de reclamación y superposición de múltiples jurisdicciones normativas internacionales.

Nivel 1: estándares Interamericanaes

Financial Action Task Force FATF/GAFI

La Recomendación 15 del FATF constituye una referencia fundamental para los activos virtuales y proveedores de servicios de activos virtuales (VASPs/ PSAV).

Nivel 2: FSB

El Financial Stability Board establece un marco global para las actividades con criptoactivos bajo el principio:

"Same activity, same risk, same regulation".

Es decir:

No debería determinarse la regulación únicamente por la tecnología utilizada, sino por la actividad económica y los riesgos que genera.

Este principio es muy útil porque permite analizar:

Blockchain → actividad económica
→ riesgo → control → regulación → evidencia.

Normativa boliviana

Resolución de Directorio BCB N.º 082/2024

El Banco Central de Bolivia mediante la Resolución de Directorio N.º 082/2024, de 25 de junio de 2024, dejó sin efecto la R.D. N.º 144/2020 y habilitó el uso de canales e Instrumentos Electrónicos de Pago para operaciones de compra y venta de activos virtuales. Esto representa un cambio fundamental respecto de la posición normativa anterior.

Por tanto, para un texto actualizado no sería correcto afirmar simplemente que "Bolivia prohíbe las criptomonedas". Debe explicarse la evolución normativa y diferenciar:

Decreto Supremo N.º 5384 de 7 de mayo de 2025

Este decreto es particularmente relevante para su investigación porque incorpora conceptos directamente relacionados con el blockchain y activos digitales.

El Decreto Supremo N.º 5384 establece un marco relacionado con Empresas de Tecnología Financiera (ETF).

Entre sus definiciones incluye:

Activo tokenizado

Representación digital de un activo real o financiero mediante tokens en blockchain.

Activo virtual

Representación digital de valor susceptible de comercialización o transferencia digital y que puede utilizarse como medio alternativo de pago o inversión, excluyendo representaciones digitales de moneda fiduciaria.

Blockchain

La norma la define como una estructura de datos compartida e inmutable para registrar transacciones y realizar seguimiento de activos mediante una red distribuida, utilizando mecanismos criptográficos y de consenso.

PSAV

Incluye actividades como:

- intercambio entre activos virtuales y moneda fiduciaria;
- intercambio entre activos virtuales;
- transferencias;
- custodia;
- administración de activos virtuales;
- servicios relacionados con la oferta o venta de activos virtuales.

Este decreto es de apoyo en la normativa boliviano.

Matriz general puede organizar los ocho subtítulos de esta manera:

Tabla No. 5

Matriz integral del ecosistema financiero digital y enfoques de auditoría forense

Tema	Tecnología Principal	Modelo de Negocio	Riesgo Principal	Área de Auditoría Forense
DeFi	Smart contracts	Préstamos, DEX, staking	Fraude / manipulación algorítmica	Análisis de contratos inteligentes y código
CBDC	DLT /	Pagos digitales y liquidación	Riesgo sistémico y operativo	Verificación de transacciones y controles institucionales
DAO	Blockchain + tokens de gobernanza	Gobernanza colectiva descentralizada	Concentración oculta de poder y votación	Auditoría de gobernanza y llaves de control (*multisig*)
Web3	Blockchain	Economía digital y propiedad soberana	Fraude digital / suplantación de propiedad	Trazabilidad de activos y flujos transaccionales
NFT	Tokens no fungibles (ERC-721/1155)	Arte, coleccionables, derechos de acceso	Falsificación, lavado y fraude especulativo	Autenticidad, metadatos y trazabilidad pericial
Tokenización	Blockchain / DLT	Fraccionamiento de activos e inversión	Discrepancia en el derecho sobre el activo subyacente	Verificación de valoración y propiedad jurídica
Stablecoins	Blockchain + reservas colaterales	Pagos y provisión de liquidez	Insuficiencia de reservas y riesgo de redención	Auditoría y verificación de respaldo financiero
Metaverso	Blockchain + realidad virtual / 3D	Bienes, inmuebles y servicios digitales	Fraude virtual, apropiación y valoración	Trazabilidad de activos digitales y avatares
P2P	Blockchain / Wallets no alojadas	Transferencia directa entre pares (*peer-to-peer*)	Incumplimiento LA/FT (AML/CFT) y anonimato	Trazabilidad de operaciones y contrapartes

Nota: las referencias bibliográficas de este capítulo se consolidaron, sin duplicados, en la sección "Bibliografía general" al final del documentos.

PARTE II

Marco Normativo, Contable y Regulatorio

4 NORMATIVIDAD INTERNACIONAL APLICABLE

4.1 Recomendaciones GAFI/FATF sobre activos virtuales

Nota terminológica: En este capítulo se utiliza la expresión activos virtuales como denominación general, conforme a la terminología empleada por el Grupo de Acción Financiera (GAFI/FATF). Cuando el contexto lo requiera, se emplearán los términos *criptoactivos* o *criptomonedas* para referirse a categorías específicas de dichos instrumentos.

La evolución de las tecnologías financieras digitales ha transformado profundamente la forma en que las personas y las organizaciones generan, almacenan y transfieren valor. Entre estas innovaciones, los activos virtuales y la tecnología blockchain han adquirido un papel protagónico en el sistema financiero global, impulsando nuevos modelos de negocio, mecanismos de inversión y sistemas descentralizados de intercambio. No obstante, el crecimiento acelerado de este ecosistema también ha incrementado la exposición a riesgos relacionados con el lavado de activos (LA), el financiamiento del terrorismo (FT) y el financiamiento de la proliferación de armas de destrucción masiva (FP), lo que ha motivado una respuesta coordinada de los organismos internacionales.

En este contexto, el Grupo de Acción Financiera (GAFI / FATF) se ha consolidado como el organismo de referencia en la formulación de estándares internacionales para la prevención del lavado de activos y el financiamiento del terrorismo (FATF, 2023). Sus recomendaciones constituyen uno de los principales referentes adoptados por las jurisdicciones soberanas para fortalecer la integridad del sistema financiero y promover una supervisión basada en riesgos. La incorporación de los activos virtuales y de los Proveedores de Servicios de Activos Virtuales (PSAV) *Virtual Asset Service Providers* (VASP) dentro del ámbito de aplicación de la Recomendación 15 representó un cambio trascendental en la regulación internacional, al reconocer que estas actividades deben estar sujetas a controles preventivos equivalentes a los exigidos a las instituciones financieras tradicionales.

Desde la perspectiva de la auditoría forense, las recomendaciones del GAFI resultan indispensables para comprender los riesgos inherentes a las operaciones con activos virtuales, diseñar procedimientos de auditoría adecuados y evaluar el cumplimiento de las obligaciones legales y regulatorias aplicables. Su implementación facilita la trazabilidad de las transacciones, fortalece los mecanismos de identificación de clientes y beneficiarios finales, y contribuye a la obtención de evidencia suficiente y apropiada en investigaciones de delitos económicos complejos.

4.2 Estándares Internacionales de Auditoría Aplicables

El Grupo de Acción Financiera (Financial Action Task Force – FATF), creado en 1989 por iniciativa del entonces Grupo de los Siete (G-7), es un organismo intergubernamental encargado de desarrollar estándares y promover la implementación efectiva de medidas legales, regulatorias y operativas destinadas a combatir el lavado de activos, el financiamiento del terrorismo y otras amenazas que afectan la integridad del sistema financiero internacional.

Las 40 Recomendaciones del GAFI, actualizadas periódicamente, constituyen el estándar internacional reconocido por organismos como el Fondo Monetario Internacional (FMI), el Banco Mundial, las Naciones Unidas y los organismos regionales de evaluación mutua. Si bien las recomendaciones no poseen carácter vinculante por sí mismas, su adopción por los Estados se ha convertido en un elemento esencial para demostrar el cumplimiento de los compromisos internacionales en materia de prevención del lavado de activos y financiamiento del terrorismo.



La incorporación de los activos virtuales dentro del ámbito regulatorio respondió al crecimiento exponencial del mercado de criptoactivos y al reconocimiento de que determinadas características de estas tecnologías como la descentralización, el alcance transfronterizo y el uso de direcciones criptográficas pueden ser utilizadas para facilitar operaciones ilícitas cuando no existen mecanismos adecuados de supervisión.

4.2.1 La Recomendación 15: Nuevas Tecnologías

La Recomendación 15 constituye uno de los principales instrumentos internacionales aplicables a los activos virtuales (FATF, 2023). Su objetivo es garantizar que las innovaciones tecnológicas no generen vulnerabilidades que puedan ser aprovechadas para actividades de lavado de activos o financiamiento del terrorismo.

En su versión vigente, la recomendación establece que los países deben identificar, evaluar y comprender los riesgos derivados de las actividades relacionadas con activos virtuales y adoptar un Enfoque Basado en Riesgo (Risk-Based Approach – RBA) para diseñar medidas proporcionales a dichos riesgos. Asimismo, exige que los Proveedores de Servicios de Activos Virtuales sean objeto de licencia o registro, supervisión efectiva y mecanismos de control que aseguren el cumplimiento de las obligaciones en materia de prevención del lavado de activos y financiamiento del terrorismo.

La Nota Interpretativa de la Recomendación 15 amplía este marco regulatorio al establecer que los PSAV deben implementar procedimientos de debida diligencia, mantener registros de las operaciones, reportar transacciones sospechosas y cooperar con las autoridades competentes. Además, introduce la denominada *Travel Rule*, que exige la obtención, conservación y transmisión de información sobre el originador y el beneficiario de determinadas transferencias de activos virtuales, fortaleciendo la trazabilidad de las operaciones y la cooperación **internacional**.

4.2.2 Activos Virtuales y Proveedores de Servicios de Activos Virtuales (PSAV)

Según el Financial Action Task Force (2023), un activo virtual es una representación digital de valor que puede comercializarse o transferirse electrónicamente y utilizarse para pagos o inversiones, excluyendo expresamente las monedas fiduciarias, los valores y otros instrumentos financieros ya regulados por otros estándares internacionales.

Por su parte, un Proveedor de Servicios de Activos Virtuales (PSAV) es toda persona física o jurídica que, como actividad comercial y por cuenta de terceros, realiza una o más de las siguientes actividades:

- Intercambio entre activos virtuales y monedas fiduciarias.
- Intercambio entre diferentes activos virtuales.
- Transferencia de activos virtuales.
- Custodia o administración de activos virtuales o de instrumentos que permitan su control.
- Participación o prestación de servicios financieros relacionados con la oferta o venta de activos virtuales.

Esta definición constituye la base para que las jurisdicciones determinen el alcance de sus sistemas de supervisión y las obligaciones regulatorias aplicables a quienes participan en el ecosistema de activos virtuales.

4.2.3 Enfoque Basado en Riesgo (Risk-Based Approach)

Uno de los principios rectores de las Recomendaciones del GAFI es la aplicación del Enfoque Basado en Riesgo (EBR), mediante el cual las medidas de prevención deben ser proporcionales al nivel de riesgo identificado.

Este enfoque exige que tanto las autoridades competentes como los PSAV desarrollen metodologías para identificar, evaluar y gestionar los riesgos asociados a sus actividades.

Entre los factores que habitualmente deben considerarse se encuentran la naturaleza y el perfil del cliente, la jurisdicción de origen o destino de las operaciones, el tipo de activo virtual involucrado, el volumen y la frecuencia de las transacciones, la utilización de tecnologías que incrementen el anonimato, los canales de distribución empleados y la complejidad de la estructura de propiedad y control.

Desde la auditoría forense, la aplicación del enfoque basado en riesgo permite orientar los procedimientos hacia aquellas operaciones con mayor probabilidad de involucrar actividades ilícitas, optimizando el uso de los recursos de auditoría y fortaleciendo la calidad de la evidencia obtenida.

4.2.1 Debida diligencia y medidas preventivas

Las Recomendaciones del GAFI establecen que los PSAV deben aplicar procedimientos de Debida Diligencia del Cliente (Customer Due Diligence – CDD) equivalentes al exigido a las instituciones financieras tradicionales.

Estas obligaciones comprenden la identificación y verificación de la identidad del cliente, la identificación del beneficiario final, la comprensión del propósito y la naturaleza de la relación comercial, el monitoreo continuo de las operaciones, la aplicación de medidas reforzadas cuando el nivel de riesgo así lo requiera, la conservación de registros durante el plazo establecido por la legislación aplicable y el reporte oportuno de operaciones sospechosas (FATF, 2023).

En conjunto, estas medidas buscan que los PSAV conozcan adecuadamente a sus clientes, documenten las operaciones realizadas y dispongan de información suficiente para colaborar con las autoridades competentes cuando sea necesario.

Asimismo, el GAFI recomienda la implementación de mecanismos tecnológicos que permitan fortalecer los procesos de identificación, monitoreo y análisis de operaciones, sin perjuicio del cumplimiento de las normas sobre protección de datos personales y privacidad.

4.2.2 La Travel Rule

Uno de los desarrollos regulatorios más relevantes derivados de la Recomendación 15 es la denominada *Travel Rule*, incorporada para reducir el anonimato en las transferencias de activos virtuales.

Esta regla exige que los PSAV obtengan, conserven y transmitan información suficiente sobre el originador y el beneficiario de determinadas operaciones, permitiendo que dicha información acompañe la transferencia durante todo su recorrido. Su finalidad es facilitar la trazabilidad de las operaciones y fortalecer la cooperación entre autoridades nacionales e internacionales en la investigación de delitos financieros.

En la práctica profesional del auditor forense, la *Travel Rule* representa una fuente relevante de evidencia, ya que facilita la reconstrucción del flujo de activos y la identificación de las personas involucradas en las transacciones.

4.2.3 Implementación de las Recomendaciones del GAFI en Iberoamérica

La incorporación de la Recomendación 15 ha impulsado importantes reformas regulatorias en los países iberoamericanos. Diversas jurisdicciones han establecido regímenes de registro o autorización para los PSAV, han fortalecido sus sistemas de supervisión y han incorporado obligaciones específicas en materia de prevención del lavado de activos y financiamiento del terrorismo.

En Paraguay, esta implementación se refleja en las resoluciones emitidas por la Secretaría de Prevención de Lavado de Dinero o Bienes (SEPRELAD), mediante las cuales los Proveedores de Servicios de Activos Virtuales fueron incorporados como sujetos obligados del sistema nacional de prevención del lavado de activos y financiamiento del terrorismo, exigiéndose su registro y la aplicación de medidas de debida diligencia acordes con los estándares internacionales. La guía sectorial de la SEPRELAD destaca que esta regulación responde a la adopción de la Recomendación 15 del GAFI y a la identificación de riesgos asociados a actividades como la minería, el intercambio, la transferencia y la custodia de activos virtuales.

4.2.4 Conclusiones

Las Recomendaciones del GAFI constituyen actualmente el principal referente internacional para la regulación de los activos virtuales y de los Proveedores de Servicios de Activos Virtuales. Su adopción ha permitido establecer estándares homogéneos orientados a reducir los riesgos asociados al lavado de activos y al financiamiento del terrorismo, promoviendo un equilibrio entre la innovación tecnológica y la integridad del sistema financiero.

Para la auditoría forense, estos estándares representan una herramienta fundamental para el diseño de procedimientos de evaluación de riesgos, la obtención de evidencia digital, el análisis de transacciones en blockchain y la verificación del cumplimiento de las obligaciones regulatorias. En consecuencia, el conocimiento y correcta aplicación de las Recomendaciones del GAFI resulta indispensable para el auditor que interviene en investigaciones relacionadas con criptoactivos, moneda digital y tecnologías de registro distribuido.

4.3 Normas Internacionales de Información Financiera (NIIF/IFRS)

4.3.1 Introducción y Marco de NIA

La transformación digital del sistema financiero ha introducido nuevos retos para la profesión contable y de auditoría, particularmente con la incorporación de activos virtuales, tecnologías de registro distribuido (Distributed Ledger Technology – DLT) y aplicaciones basadas en blockchain. Estas innovaciones modifican la forma en que las organizaciones generan, registran, custodian y transfieren valor, obligando a los auditores a adaptar sus procedimientos sin apartarse de los principios fundamentales establecidos por las Normas Internacionales de Auditoría (NIA), emitidas por el International Auditing and Assurance Standards Board (IAASB, 2023).

Aunque el IAASB aún no ha emitido una norma específica para la auditoría de activos virtuales, el conjunto de las NIA proporciona un marco metodológico suficiente para planificar, ejecutar y documentar auditorías que involucren este tipo de activos. La aplicación de estas normas requiere que el auditor complemente sus conocimientos contables con competencias en tecnologías digitales, ciberseguridad, análisis de datos y funcionamiento de redes blockchain, manteniendo siempre el escepticismo profesional y el juicio crítico que caracterizan la actividad de auditoría.

Para el profesional encargado de la investigación, la correcta aplicación de las NIA permite obtener evidencia suficiente y apropiada para evaluar la existencia, integridad, valuación, titularidad y trazabilidad de los activos virtuales, así como detectar posibles esquemas de fraude, lavado de activos, financiamiento del terrorismo u otras conductas ilícitas.

4.3.2 Aplicación de las Normas Internacionales de Auditoría en el ecosistema de activos virtuales

Las NIA constituyen un conjunto integrado de principios y procedimientos que orientan el trabajo del auditor independiente. Su aplicación no depende del tipo de activo auditado, sino de los riesgos que afectan la razonabilidad de la información financiera. En consecuencia, las operaciones con activos virtuales deben evaluarse bajo los mismos principios de independencia, competencia profesional, planificación, obtención de evidencia y documentación exigidos para cualquier otra auditoría.

Sin embargo, las particularidades tecnológicas de los criptoactivos demandan procedimientos adicionales orientados a comprender el funcionamiento de las plataformas utilizadas, verificar la autenticidad de las transacciones registradas en *blockchain* y evaluar los riesgos asociados a la custodia de claves criptográficas, contratos inteligentes (*smart contracts*) y servicios prestados por terceros.

Tabla No. 6

Aplicación de las Normas Internacionales de Auditoría en la auditoría de activos virtuales

Norma NIA	Foco Normativo	Aplicación en Auditoría Forense y de Activos Virtuales
NIA 200	Objetivos globales del auditor independiente	Verificar la existencia de activos, control de wallets, medición contable y suficiencia de revelaciones en estados financieros.
NIA 240	Responsabilidad del auditor respecto al fraude	Evaluar riesgos de incorrección material por fraude derivados de seudónimo, mixers, smart contracts maliciosos y ocultación de activos.
NIA 250	Consideración de disposiciones legales y reglamentarias	Evaluar el cumplimiento de normas LA/FT (SEPRELAD/GAFI), licencias PSAV, obligaciones tributarias y normativas de protección de datos.
NIA 315	Identificación y valoración de riesgos	Analizar la infraestructura tecnológica, tipos de blockchain, mecanismos de consenso, custodia (hot/cold wallets) y gobernanza IT.
NIA 330	Respuestas del auditor a los riesgos valorados	Diseñar pruebas sustantivas, conciliaciones contables-blockchain, confirmaciones criptográficas y revisión de controles de acceso.
NIA 500	Evidencia de auditoría	Obtener evidencia suficiente mediante registros distribuidos, hashes, exploradores de bloques y documentos de identificación de clientes.
NIA 520	Procedimientos analíticos	Aplicar analítica de datos para detectar patrones inusuales, transacciones fraccionadas, picos de liquidez y flujos hacia jurisdicciones de riesgo.
NIA 530	Muestreo de auditoría	Seleccionar partidas o evaluar la totalidad de las transacciones (población completa en blockchain) aplicando juicio profesional.

Norma NIA	Foco Normativo	Aplicación en Auditoría Forense y de Activos Virtuales
NIA 550	Partes relacionadas	Identificar relaciones ocultas y control simultáneo de múltiples direcciones blockchain por una misma contraparte o beneficiario final.

Fuente: Elaboración propia con base en las Normas **Internacionales** *de Auditoría emitidas por el International Auditing and Assurance Standards Board (IAASB, 2023).*

4.3.3 NIA 200 – Objetivos globales del auditor independiente

La NIA 200 establece que el objetivo del auditor consiste en obtener una seguridad razonable de que los estados financieros están libres de incorrecciones materiales (IAASB, 2023). En el ámbito de los activos virtuales, este objetivo implica verificar la existencia de los activos registrados, la titularidad o el control efectivo sobre las billeteras digitales, la adecuada clasificación contable, la correcta medición inicial y posterior, la integridad de las transacciones y la suficiencia de las revelaciones efectuadas en los estados financieros.

Para ello, el auditor debe comprender no solo el modelo de negocio de la entidad, sino también la infraestructura tecnológica utilizada para administrar los activos virtuales.

4.3.4 NIA 240 – Responsabilidad del auditor respecto al fraude

La NIA 240 requiere que el auditor identifique y valore los riesgos de incorrección material derivados del fraude, manteniendo un adecuado nivel de escepticismo profesional durante toda la auditoría.

Las operaciones con activos virtuales presentan riesgos particulares asociados al anonimato o pseudonimato de los participantes, la utilización de múltiples direcciones *blockchain*, la apropiación indebida de claves privadas, la manipulación de contratos inteligentes (*smart contracts*), el uso de plataformas descentralizadas (DeFi) y el empleo de servicios destinados a dificultar la trazabilidad de las operaciones.

En consecuencia, el auditor deberá diseñar procedimientos específicos para evaluar si estas características han sido utilizadas para ocultar transacciones ilícitas o distorsionar la información financiera.

4.3.5 NIA 250 – Consideración de las disposiciones legales y reglamentarias

La NIA 250 dispone que el auditor debe considerar el efecto de las disposiciones legales y reglamentarias aplicables sobre los estados financieros y sobre la auditoría.

En materia de activos virtuales, ello implica evaluar el cumplimiento de la normativa relacionada con la prevención del lavado de activos y del financiamiento del terrorismo, las obligaciones tributarias, la protección de datos personales, los requisitos aplicables al licenciamiento o registro de los Proveedores de Servicios de Activos Virtuales (PSAV) y los requerimientos de información establecidos por las autoridades competentes.

Asimismo, el auditor debe mantenerse actualizado respecto de la evolución normativa de cada jurisdicción, considerando que la regulación de los activos virtuales continúa desarrollándose de forma dinámica.

4.3.6 NIA 315 (Revisada) – Identificación y valoración de riesgos

La NIA 315 (Revisada) exige que el auditor obtenga un conocimiento suficiente de la entidad y de su entorno para identificar y valorar los riesgos de incorrección material (IAASB, 2023).

En auditorías relacionadas con activos virtuales, este análisis comprende el tipo de *blockchain* utilizada, los mecanismos de consenso implementados, las políticas para la administración de claves criptográficas, los procedimientos de custodia de activos, el uso de billeteras frías (*cold wallets*) y calientes (*hot wallets*), la dependencia de proveedores externos, los controles de ciberseguridad existentes y la gobernanza tecnológica de la organización.

La adecuada comprensión de estos elementos constituye la base para determinar la naturaleza, oportunidad y extensión de los procedimientos de auditoría.

4.3.7 NIA 330 – Respuestas del auditor a los riesgos valorados

Una vez identificados los riesgos, la NIA 330 exige que el auditor diseñe respuestas apropiadas para obtener evidencia suficiente y adecuada.

En operaciones con activos virtuales, estas respuestas pueden comprender la conciliación entre los registros contables y la información disponible en la *blockchain*, la confirmación de saldos mediante evidencia criptográfica, la revisión de los controles de acceso a billeteras digitales, el análisis de transacciones mediante herramientas especializadas y la evaluación de la seguridad informática relacionada con la custodia de los activos digitales.

La selección de estos procedimientos dependerá de la naturaleza y magnitud de los riesgos previamente identificados, así como de la complejidad de las operaciones realizadas por la entidad.

4.3.8 NIA 500 – Evidencia de auditoría

La NIA 500 dispone que la evidencia obtenida debe ser suficiente y apropiada para sustentar la opinión del auditor (IAASB, 2023).

En el entorno *blockchain*, la evidencia puede obtenerse a partir de registros distribuidos, hashes criptográficos, direcciones públicas, exploradores de *blockchain*, registros generados por plataformas de intercambio, contratos inteligentes y documentación relacionada con la custodia de los activos digitales.

No obstante, la existencia de una transacción registrada en *blockchain* no demuestra por sí sola la identidad del titular económico de los activos, razón por la cual esta evidencia debe complementarse con procedimientos de identificación del cliente, verificación documental y análisis del beneficiario final.

4.3.9 NIA 520 – Procedimientos analíticos

Los procedimientos analíticos previstos por la NIA 520 adquieren especial relevancia en auditorías de activos virtuales debido al elevado volumen de información disponible en las cadenas de bloques.

El empleo de herramientas de análisis de datos permite identificar patrones inusuales de comportamiento, operaciones repetitivas, transacciones fraccionadas, movimientos entre billeteras relacionadas, transferencias hacia jurisdicciones de alto riesgo y concentraciones significativas de operaciones. El análisis conjunto de estos indicadores fortalece la identificación de riesgos y complementa los procedimientos sustantivos tradicionales, especialmente en investigaciones que involucran grandes volúmenes de transacciones registradas en *blockchain*.

4.3.10 NIA 530 – Muestreo de auditoría

Aunque la tecnología *blockchain* permite acceder a la totalidad de las transacciones registradas, ello no elimina la necesidad del juicio profesional en la selección de procedimientos.

Dependiendo de la naturaleza de la auditoría y del volumen de operaciones, el auditor podrá revisar la totalidad de las transacciones relevantes o aplicar técnicas de muestreo orientadas hacia aquellas operaciones que presenten un mayor riesgo de incorrección material.

4.3.11 NIA 550 – Partes relacionadas

La NIA 550 requiere que el auditor identifique operaciones con partes relacionadas que puedan afectar la razonabilidad de la información financiera.

En el ecosistema de activos virtuales este análisis reviste especial importancia debido a la posibilidad de que una misma persona controle múltiples direcciones *blockchain* sin que dicha relación resulte evidente.

Por ello, el auditor deberá complementar la revisión documental con procedimientos destinados a identificar beneficiarios finales, estructuras de control y relaciones económicas entre las partes involucradas.

4.3.12 Consideraciones para la auditoría forense

La auditoría forense de activos virtuales exige integrar los principios establecidos por las Normas Internacionales de Auditoría con herramientas especializadas de análisis tecnológico. La utilización de exploradores *blockchain*, plataformas de análisis de transacciones, técnicas de preservación de evidencia digital y procedimientos de trazabilidad permite fortalecer la calidad de la evidencia obtenida y mejorar la capacidad del auditor para reconstruir operaciones complejas. En este contexto, el juicio profesional adquiere una relevancia particular, ya que la evidencia tecnológica debe ser evaluada conjuntamente con la información contable, documental y legal disponible, garantizando que las conclusiones alcanzadas sean objetivas, verificables y técnicamente fundamentadas.

Las Normas Internacionales de Auditoría proporcionan un marco suficientemente flexible para responder a los desafíos que plantea el ecosistema de los activos virtuales. Aunque ninguna de ellas fue concebida específicamente para la auditoría de criptoactivos, sus principios permiten adaptar los procedimientos de auditoría a los riesgos tecnológicos, operativos y regulatorios propios de

este entorno. En consecuencia, el auditor debe complementar el conocimiento de las NIA con competencias en *blockchain*, análisis de datos y evidencia digital, fortaleciendo así la calidad del juicio profesional y la confiabilidad de las conclusiones alcanzadas.

4.3.13 Consideraciones metodológicas para la auditoría forense

La auditoría forense de activos virtuales exige integrar los principios establecidos por las Normas **Internacionales** de Auditoría con herramientas tecnológicas especializadas. La utilización de exploradores blockchain, plataformas de análisis de transacciones, técnicas de preservación de evidencia digital y procedimientos de trazabilidad permite fortalecer la calidad de la evidencia obtenida y mejorar la capacidad del auditor para reconstruir operaciones complejas.

En este contexto, el juicio profesional adquiere una relevancia particular, ya que la evidencia tecnológica debe ser evaluada conjuntamente con la información contable, documental y legal disponible, garantizando que las conclusiones alcanzadas sean objetivas, verificables y técnicamente fundamentadas.

Las Normas Internacionales de Auditoría proporcionan un marco suficientemente flexible para responder a los desafíos que plantea el ecosistema de los activos virtuales. Aunque ninguna de ellas fue concebida específicamente para la auditoría de criptoactivos, sus principios permiten adaptar los procedimientos de auditoría a los riesgos tecnológicos, operativos y regulatorios propios de este entorno. En consecuencia, el auditor debe complementar el conocimiento de las NIA con competencias en blockchain, análisis de datos y evidencia digital, fortaleciendo así la calidad del juicio profesional y la confiabilidad de las conclusiones alcanzadas.

4.4 Normas Internacionales de Información Financiera (NIIF / IFRS)

4.4.1 Introducción

El crecimiento sostenido de los activos virtuales ha generado importantes desafíos para la información financiera, especialmente en lo relacionado con su reconocimiento, medición, presentación y revelación en los estados financieros. A diferencia de otros activos financieros tradicionales, los criptoactivos presentan características particulares derivadas de su naturaleza digital, descentralizada y criptográfica, lo que ha motivado un amplio debate respecto de su adecuado tratamiento contable bajo las Normas Internacionales de Información Financiera (NIIF/IFRS).

Hasta la fecha, el International Accounting Standards Board (IASB) no ha emitido una norma específica aplicable a los activos virtuales (IFRS Foundation, 2024). En consecuencia, las entidades deben analizar las características económicas de cada tipo de activo digital para determinar el tratamiento contable más apropiado, aplicando las normas existentes de manera consistente con los principios generales establecidos en el Marco Conceptual para la Información Financiera.

El IFRS Interpretations Committee (IFRIC) ha señalado que, en la mayoría de los casos, las criptomonedas no cumplen la definición de efectivo ni de equivalente de efectivo y, salvo circunstancias particulares, tampoco reúnen las características de un instrumento financiero. Por ello, su tratamiento contable dependerá de la finalidad para la cual sean mantenidas por la entidad y de los derechos económicos que incorporen.

En el desarrollo de una auditoría especializada, la adecuada aplicación de las NIIF resulta fundamental para verificar la correcta clasificación de los activos virtuales, evaluar la razonabilidad de su medición y determinar si las revelaciones contenidas en los estados financieros reflejan adecuadamente los riesgos asociados a este tipo de activos.

4.4.2 Marco Conceptual para la Información Financiera

El Marco Conceptual para la Información Financiera constituye la base para la elaboración y aplicación de las NIIF (IFRS Foundation, 2018). En ausencia de una norma específica sobre activos virtuales, este documento adquiere espe-

cial relevancia, ya que orienta el juicio profesional en la selección de políticas contables apropiadas.

De acuerdo con el Marco Conceptual, un activo es un recurso económico presente controlado por la entidad como resultado de sucesos pasados, del cual se espera obtener beneficios económicos futuros. En este sentido, los activos virtuales pueden cumplir la definición de activo cuando la entidad ejerce control sobre ellos, generalmente mediante la posesión y administración de las claves criptográficas que permiten disponer de dichos activos.

Asimismo, el Marco Conceptual exige que la información financiera represente fielmente la realidad económica de las transacciones, lo que implica que el tratamiento contable de los activos virtuales debe responder a su sustancia económica y no únicamente a su forma jurídica (IFRS Foundation, 2018).

4.4.3 Pronunciamiento del IFRS Interpretations Committee

En junio de 2019, el IFRS Interpretations Committee emitió una decisión de agenda sobre la contabilización de las tenencias de criptomonedas (Holdings of Cryptocurrencies), concluyendo que, en términos generales, las criptomonedas deben contabilizarse como activos intangibles conforme a la NIC 38, salvo que sean mantenidas para su venta en el curso ordinario del negocio, caso en el cual resulta aplicable la NIC 2 Inventarios (IFRS Interpretations Committee, 2019).

Esta interpretación constituye actualmente uno de los principales referentes internacionales para el tratamiento contable de los criptoactivos bajo las Normas Internacionales de Información Financiera (NIIF) y ha sido ampliamente considerada por entidades, auditores y organismos reguladores en distintas jurisdicciones (IFRS Interpretations Committee, 2019).

4.4.4 NIC 38 – Activos Intangibles

La NIC 38 establece los criterios para el reconocimiento, medición y revelación de los activos intangibles.

En términos generales, las criptomonedas mantenidas como inversión o reserva de valor reúnen las características de un activo intangible, al tratarse de recursos identificables, carentes de sustancia física, controlados por la entidad y capaces de generar beneficios económicos futuros (IFRS Foundation, 2024).

De conformidad con esta norma, el reconocimiento inicial debe efectuarse al costo, mientras que la medición posterior podrá realizarse mediante el modelo del costo o, cuando exista un mercado activo, mediante el modelo de revaluación.

Desde la auditoría forense, el profesional deberá verificar la existencia del mercado activo utilizado para la medición, la consistencia del criterio aplicado y la adecuada documentación de las variaciones de valor.

4.4.5 NIC 2 – Inventarios

Cuando una entidad mantiene activos virtuales con la finalidad de venderlos en el curso ordinario de sus operaciones, dichos activos deben contabilizarse como inventarios conforme a la NIC 2.

Este tratamiento resulta habitual en entidades cuya actividad principal consiste en la intermediación o comercialización de criptoactivos, tales como determinados exchanges o corredores especializados.

En estos casos, la medición se realizará conforme a las disposiciones establecidas para inventarios, considerando las particularidades previstas para intermediarios de materias primas cuando resulten aplicables (IFRS Foundation, 2024).

4.4.6 NIIF 13 – Medición del Valor Razonable

La NIIF 13 proporciona el marco para determinar el valor razonable cuando otra norma exige o permite dicha medición.

En el contexto de los activos virtuales, esta norma adquiere especial importancia debido a la elevada volatilidad de los precios de mercado y a la existencia de múltiples plataformas de negociación.

En consecuencia, el auditor deberá evaluar la existencia de mercados activos, la jerarquía del valor razonable utilizada, la consistencia de las fuentes de información empleadas y la razonabilidad de las técnicas de valoración cuando no existan precios observables (IFRS Foundation, 2024).

La adecuada determinación del valor razonable resulta esencial para garantizar la comparabilidad y transparencia de la información financiera.

4.4.7 NIC 1 – Presentación de Estados Financieros

La NIC 1 establece los principios generales para la presentación de los estados financieros y exige que la información sea relevante, fiable y comprensible para los usuarios.

En relación con los activos virtuales, la entidad deberá revelar, entre otros aspectos:

- Políticas contables aplicadas.
- Criterios de clasificación.
- Bases de medición.
- Riesgos asociados.
- Juicios significativos realizados por la administración.
- Incertidumbres relacionadas con la valoración.

Estas revelaciones contribuyen a mejorar la transparencia y permiten a los usuarios comprender el impacto económico de las operaciones con activos virtuales.

4.4.8 NIC 8 – Políticas Contables, Cambios en las Estimaciones Contables y Errores

La NIC 8 adquiere especial relevancia debido a la inexistencia de una NIIF específica para activos virtuales.

Esta norma establece que, cuando una transacción no esté regulada por una NIIF particular, la administración deberá ejercer juicio profesional para desarrollar y aplicar una política contable que proporcione información relevante y fiable, considerando el Marco Conceptual y otras normas relacionadas.

En consecuencia, las políticas adoptadas para el reconocimiento y medición de activos virtuales deberán aplicarse de manera consistente y divulgarse adecuadamente en las notas a los estados financieros.

4.4.9 Implicancias para la auditoría forense

La clasificación contable de los activos virtuales constituye uno de los principales aspectos que deben ser evaluados durante una auditoría forense.

En el desarrollo de una auditoría forense, el profesional deberá verificar que la clasificación contable adoptada sea consistente con la finalidad económica del activo virtual, que la medición se encuentre sustentada en información verificable, que las políticas contables hayan sido aplicadas de manera uniforme y

que las revelaciones efectuadas permitan comprender adecuadamente los riesgos asociados a estos activos. Asimismo, deberá obtener evidencia suficiente respecto de la titularidad y del control ejercido sobre los activos virtuales.

De igual forma, será necesario considerar los riesgos derivados de la volatilidad del mercado, la posible pérdida o compromiso de las claves criptográficas, la utilización de custodios externos y las limitaciones existentes para determinar el valor razonable en mercados con escasa liquidez.

4.4.10 Conclusiones

La inexistencia de una Norma Internacional de Información Financiera específicamente dedicada a los activos virtuales ha llevado a que su tratamiento contable se construya a partir de la aplicación sistemática de normas ya existentes, principalmente la NIC 38 y la NIC 2, complementadas por el Marco Conceptual, la NIIF 13, la NIC 1 y la NIC 8. Este enfoque refleja la naturaleza dinámica del ecosistema digital y exige que los profesionales documenten adecuadamente el juicio aplicado al seleccionar las políticas contables más apropiadas para cada operación.

Para la auditoría forense, la correcta aplicación de estas normas resulta esencial para evaluar la razonabilidad de la clasificación, medición y revelación de los activos virtuales, así como para detectar posibles incorrecciones materiales derivadas de errores, fraude o interpretaciones inadecuadas de las políticas contables.

Tabla No. 7

Normas Internacionales de Información Financiera aplicables al tratamiento contable de los activos virtuales

Norma	Aspecto regulado	Aplicación a los activos virtuales
Marco Conceptual	Definición y reconocimiento de activos	Determina si el activo virtual cumple la definición de activo.
NIC 38	Activos intangibles	Aplicable a criptomonedas mantenidas como inversión o reserva de valor.
NIC 2	Inventarios	Aplicable cuando los activos virtuales se mantienen para su venta en el curso ordinario del negocio.
NIIF 13	Medición del valor razonable	Determina los criterios para medir activos virtuales cuando procede el valor razonable.

Norma	Aspecto regulado	Aplicación a los activos virtuales
NIC 1	Presentación de estados financieros	Exige la adecuada presentación y revelación de políticas contables y riesgos asociados.
NIC 8	Políticas contables	Orienta el desarrollo de políticas contables ante la ausencia de una NIIF específica sobre activos virtuales.

Nota. *Elaboración propia con base en el Marco Conceptual para la Información Financiera (IFRS Foundation, 2018), las Issued IFRS Accounting Standards (IFRS Foundation, 2024) y la decisión de agenda Holdings of Cryptocurrencies (IFRS Interpretations Committee, 2019).*

4.5 Regulación Comparada en Iberoamérica

4.5.1 Introducción

La expansión del mercado de activos virtuales ha motivado que numerosos países de Iberoamérica desarrollen marcos regulatorios destinados a fortalecer la seguridad jurídica, promover la innovación tecnológica y mitigar los riesgos asociados al lavado de activos, el financiamiento del terrorismo, la evasión fiscal y la protección de los inversionistas. Sin embargo, la velocidad de evolución de las tecnologías basadas en *blockchain* ha generado importantes diferencias en el grado de desarrollo normativo entre las distintas jurisdicciones.

En términos generales, los países iberoamericanos han seguido las recomendaciones emitidas por el Grupo de Acción Financiera Internacional (GAFI/FATF), especialmente aquellas relacionadas con el registro o autorización de los Proveedores de Servicios de Activos Virtuales (PSAV), la implementación de medidas de debida diligencia y la adopción de enfoques basados en riesgo. No obstante, el tratamiento jurídico de los activos virtuales continúa siendo heterogéneo, particularmente en aspectos vinculados a la supervisión financiera, la tributación y el reconocimiento contable.

El análisis comparado permite identificar tendencias regulatorias comunes y constituye una herramienta útil para auditores, contadores y peritos forenses que intervienen en operaciones transfronterizas o investigaciones relacionadas con activos digitales.

4.5.2 España

España ha desarrollado uno de los marcos regulatorios más avanzados de la región, alineado con la normativa de la Unión Europea. La regulación de los proveedores de servicios de activos virtuales se encuentra orientada a la prevención del lavado de activos, estableciendo obligaciones de registro, identificación de clientes y reporte de operaciones sospechosas.

Asimismo, la legislación española incorpora obligaciones tributarias específicas para la declaración de criptoactivos y participa en la implementación del Reglamento sobre Mercados de Criptoactivos (*Markets in Crypto-Assets Regulation – MiCA*), que establece un régimen armonizado para los Estados miembros de la Unión Europea (Parlamento Europeo y Consejo de la Unión Europea, 2023)s.

4.5.3 Portugal

Portugal ha mantenido una política orientada al desarrollo del ecosistema tecnológico y la innovación financiera, complementándola progresivamente con medidas regulatorias en materia de prevención del lavado de activos y supervisión de proveedores de servicios de activos virtuales. La evolución normativa reciente ha fortalecido las obligaciones de registro, transparencia y cooperación con las autoridades competentes, alineándose tanto con las recomendaciones del Grupo de Acción Financiera Internacional (FATF, 2023) como con el marco regulatorio de la Unión Europea aplicable a los mercados de criptoactivos (Parlamento Europeo y Consejo de la Unión Europea, 2023)s.

4.5.4 Brasil

Brasil constituye una de las jurisdicciones más desarrolladas de América Latina en materia de regulación de activos virtuales. La aprobación de la Ley Nº 14.478/2022 estableció un marco jurídico para los prestadores de servicios de activos virtuales, definiendo principios generales para su funcionamiento y asignando competencias regulatorias a las autoridades nacionales (Brasil, Ley Nº 14.478/2022).

El modelo brasileño combina la promoción de la innovación tecnológica con mecanismos de supervisión prudencial, prevención del lavado de activos

y protección del consumidor, consolidándose como una referencia para otros países de la regións.

4.5.5 Argentina

Argentina presenta un mercado de activos virtuales de significativa expansión, impulsado por factores económicos y financieros internos. Aunque aún no dispone de una ley integral sobre criptoactivos, diversas autoridades han emitido regulaciones relacionadas con la prevención del lavado de activos, el tratamiento tributario y la supervisión de determinadas actividades vinculadas al ecosistema digital.

En los últimos años se ha fortalecido la coordinación entre organismos financieros, tributarios y de prevención del lavado de activos para incrementar la transparencia de las operaciones con activos virtuales.

4.5.6 Colombia

Colombia ha optado por un modelo de regulación progresiva basado en programas piloto y espacios de innovación regulatoria (*sandbox*), permitiendo evaluar el funcionamiento de servicios relacionados con activos virtuales antes de su regulación definitiva.

Paralelamente, las autoridades han emitido lineamientos dirigidos a fortalecer la prevención del lavado de activos y promover la cooperación entre el sector financiero tradicional y las empresas dedicadas al desarrollo de tecnologías financieras.

4.5.7 Chile

Chile ha incorporado progresivamente disposiciones aplicables a los proveedores de servicios financieros basados en tecnologías digitales mediante la denominada Ley Fintech, fortaleciendo la supervisión de determinadas actividades vinculadas con activos virtuales y promoviendo la innovación dentro de un marco de estabilidad financiera.

La regulación chilena prioriza la transparencia, la protección de los usuarios y la gestión adecuada de riesgos operacionales y tecnológicos.

4.5.8 Ecuador

En Ecuador, el uso de activos virtuales no constituye moneda de curso legal, manteniéndose el dólar estadounidense como única moneda oficial. No obstante, la utilización de criptoactivos como bienes digitales no se encuentra prohibida, siempre que las operaciones respeten el marco jurídico vigente.

Las autoridades han emitido pronunciamientos orientados a advertir sobre los riesgos asociados a este tipo de activos y continúan desarrollando mecanismos regulatorios compatibles con las recomendaciones internacionales en materia de prevención del lavado de activos.

4.5.9 Paraguay

En Paraguay, el desarrollo regulatorio de los activos virtuales se ha concentrado principalmente en el ámbito de la prevención del lavado de activos y del financiamiento del terrorismo. La Secretaría de Prevención de Lavado de Dinero o Bienes (SEPRELAD) incorporó a los Proveedores de Servicios de Activos Virtuales como sujetos obligados del sistema nacional de prevención, exigiendo su registro y la implementación de procedimientos de debida diligencia acordes con las recomendaciones internacionales (Secretaría de Prevención de Lavado de Dinero o Bienes [SEPRELAD], 2020). Estas medidas fueron precedidas por un estudio sectorial que identificó los riesgos específicos del ecosistema de activos virtuales en el país.

La doctrina nacional también ha señalado que el desarrollo normativo paraguayo en materia de activos virtuales ha evolucionado principalmente desde la perspectiva de la prevención del lavado de activos y del financiamiento del terrorismo, mientras que otros aspectos, como la regulación integral del mercado de criptoactivos, continúan en proceso de consolidación (Vouga Abogados, 2022).

En el ámbito tributario, la **Dirección Nacional de Ingresos Tributarios (DNIT)** ha incorporado mecanismos de control e intercambio de información relacionados con operaciones que involucran activos virtuales, fortaleciendo la transparencia fiscal y alineándose con los estándares internacionales (Dirección Nacional de Ingresos Tributarios [DNIT], 2026; Banco Central del Paraguay [BCP], s. f.). Por su parte, el **Banco Central del Paraguay (BCP)** ha reiterado que las criptomonedas no constituyen moneda de curso legal ni cuentan con respaldo del banco central, advirtiendo sobre los riesgos inherentes a su utilización. Estas actuaciones evidencian una regulación sectorial que, aunque aún

no configura una ley integral sobre criptoactivos, refleja una implementación progresiva de los estándares internacionales.

4.5.10 Tendencias regulatorias comunes en Iberoamérica

Del análisis comparado pueden identificarse diversas tendencias compartidas por las jurisdicciones iberoamericanas:

- adopción de las Recomendaciones del GAFI como referencia para la regulación de los PSAV;
- fortalecimiento de los sistemas de prevención del lavado de activos y financiamiento del terrorismo;
- incorporación gradual de obligaciones tributarias relacionadas con activos virtuales;
- desarrollo de mecanismos de supervisión especializados para proveedores de servicios de activos virtuales;
- promoción de la innovación tecnológica mediante marcos regulatorios flexibles y espacios de prueba (*sandbox regulatorios*);

incremento de la cooperación internacional e intercambio de información entre autoridades competentes.

Estas tendencias evidencian un proceso de convergencia regulatoria, aunque persisten diferencias significativas en cuanto al alcance y nivel de desarrollo de las legislaciones nacionales.

4.5.11 Implicancias para la auditoría forense

La diversidad normativa existente en Iberoamérica exige que el auditor forense adopte un enfoque multidisciplinario y considere las particularidades regulatorias de cada jurisdicción involucrada en la operación objeto de análisis.

Las investigaciones relacionadas con activos virtuales frecuentemente presentan componentes transfronterizos, por lo que resulta indispensable evaluar la legislación aplicable, las obligaciones de los proveedores de servicios de activos virtuales y los mecanismos de cooperación internacional disponibles para la obtención de evidencia.

En este contexto, el conocimiento comparado de los distintos marcos regulatorios fortalece la capacidad del auditor para interpretar adecuadamente las operaciones analizadas, valorar los riesgos asociados y emitir conclusiones técnicamente fundamentadas.

4.5.12 Conclusiones

La regulación de los activos virtuales en Iberoamérica continúa en un proceso de evolución permanente. Aunque existen diferencias entre las distintas jurisdicciones, puede observarse una tendencia común hacia la adopción de estándares internacionales orientados a fortalecer la transparencia, la prevención del lavado de activos, la protección de los usuarios y la supervisión de los proveedores de servicios de activos virtuales.

La convergencia progresiva de estos marcos regulatorios facilita la cooperación internacional y proporciona a los auditores forenses un contexto normativo más uniforme para el análisis de operaciones con activos virtuales, sin perjuicio de la necesidad de considerar las particularidades legales de cada país.

Tabla No. 8

Comparación de los principales enfoques regulatorios sobre activos virtuales en Iberoamérica

País	Enfoque regulatorio predominante	Aspectos relevantes
España	Regulación integral alineada con MiCA	Registro de PSAV, prevención del LA/FT y obligaciones tributarias.
Portugal	Supervisión y registro de PSAV	Enfoque compatible con la normativa de la Unión Europea.
Brasil	Marco legal específico	Ley Nº 14.478/2022 para prestadores de servicios de activos virtuales.
Argentina	Regulación sectorial	Medidas tributarias y de prevención del lavado de activos.
Colombia	Regulación progresiva	Programas piloto (*sandbox*) y lineamientos para innovación financiera.
Chile	Ley Fintech	Supervisión de servicios financieros tecnológicos y gestión de riesgos.
Ecuador	Regulación parcial	Advertencias regulatorias y aplicación de normas generales.
Paraguay	Regulación sectorial	SEPRELAD (PSAV y prevención del LA/FT), DNIT (control tributario) y BCP (advertencias sobre criptoactivos).

Nota. *Elaboración propia con base en las Recomendaciones del GAFI (FATF, 2023), el Reglamento (UE) 2023/1114 (MiCA), la Ley Nº 14.478/2022 de Brasil y la normativa oficial vigente de las autoridades competentes de las jurisdicciones analizadas.*

4.6 Directrices OCDE y organismos multilaterales

4.6.1 Introducción

La expansión de los activos virtuales ha generado nuevos desafíos para la transparencia fiscal internacional, la estabilidad financiera, la protección de los inversionistas y la cooperación entre autoridades. Por ello, distintos organismos multilaterales han emitido directrices orientadas a establecer criterios comunes para la supervisión, el intercambio de información y la gestión de riesgos asociados a criptoactivos, moneda digital y tecnología *blockchain*.

En este contexto, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) ocupa un lugar central mediante el desarrollo del **Crypto-Asset Reporting Framework (CARF)** y las modificaciones al **Common Reporting Standard (CRS)**, instrumentos destinados a facilitar el intercambio automático de información tributaria (Organisation for Economic Co-operation and Development [OECD], 2022). La OCDE publicó el marco final del CARF y las enmiendas al CRS en 2022, y posteriormente estos estándares fueron incorporados al marco internacional de intercambio automático de información tributaria.

Desde la auditoría forense, estas directrices permiten comprender cómo las operaciones con activos virtuales pueden ser objeto de trazabilidad fiscal, identificación de usuarios, reconstrucción de operaciones y cooperación administrativa internacional.

4.6.2 OCDE y transparencia fiscal internacional

La OCDE ha desarrollado estándares internacionales orientados a combatir la evasión fiscal y mejorar la cooperación entre administraciones tributarias. En materia de activos virtuales, su principal aporte es el **Crypto-Asset Reporting Framework (CARF)**, diseñado para que los proveedores de servicios relacionados con criptoactivos reporten información relevante a las autoridades fiscales de sus respectivas jurisdicciones.

El CARF busca cubrir operaciones que, por su naturaleza descentralizada o transfronteriza, podían quedar fuera de los mecanismos tradicionales de intercambio de información financiera. Entre las operaciones reportables se incluyen intercambios entre criptoactivos y moneda fiduciaria, intercambios entre distintos criptoactivos y transferencias de criptoactivos.

Este marco complementa al **Common Reporting Standard (CRS)**, que desde 2014 ha constituido el estándar internacional de intercambio automático de

información sobre cuentas financieras. Las modificaciones introducidas al CRS buscan ampliar su alcance frente a nuevos productos financieros digitales, incluyendo determinados activos electrónicos y monedas digitales.

4.6.3 Crypto-Asset Reporting Framework (CARF)

El CARF establece un sistema de debida diligencia, identificación y reporte aplicable a intermediarios y proveedores de servicios de criptoactivos. Su finalidad es que las autoridades tributarias puedan recibir información estructurada sobre usuarios, operaciones y saldos relevantes (OECD, 2022); reduciendo los espacios de opacidad fiscal derivados del uso de activos virtuales.

Para la auditoría forense, el CARF resulta especialmente relevante porque incorpora estándares de documentación y reporte que facilitan la identificación de usuarios de plataformas, la reconstrucción de operaciones transfronterizas, el análisis de ganancias, pérdidas y demás eventos con incidencia tributaria, el contraste entre la información contable, fiscal y la registrada en *blockchain*, así como la detección de operaciones que no hayan sido oportunamente declaradas ante las autoridades competentes.

En la práctica, el CARF fortalece la relación entre fiscalidad digital, trazabilidad tecnológica y cooperación internacionals.

4.6.4 Common Reporting Standard (CRS) y activos digitales

El CRS fue diseñado para el intercambio automático de información financiera entre jurisdicciones, con el objetivo de combatir la evasión fiscal internacional. Sin embargo, el crecimiento de los activos virtuales exigió su actualización, ya que muchos criptoactivos no eran mantenidos necesariamente en instituciones financieras tradicionales.

Las modificaciones al CRS buscan incorporar nuevos productos financieros digitales y evitar que la innovación tecnológica sea utilizada para eludir obligaciones fiscales. En este sentido, el CRS actualizado y el CARF deben interpretarse como instrumentos complementarios: el primero enfocado en cuentas financieras tradicionales y determinadas formas digitales asimilables, y el segundo orientado específicamente a criptoactivos.

4.6.5 Fondo Monetario Internacional y Junta de Estabilidad Financiera

El Fondo Monetario Internacional (FMI) y la Junta de Estabilidad Financiera (*Financial Stability Board* – FSB) han abordado los activos virtuales desde la perspectiva de la estabilidad financiera, la política monetaria y la integridad del sistema financiero.

En 2023, el FMI y la FSB publicaron un documento de síntesis sobre políticas para criptoactivos, elaborado a solicitud del G20, con el propósito de establecer una hoja de ruta coordinada para responder a los riesgos macroeconómicos y financieros derivados del ecosistema cripto (International Monetary Fund & Financial Stability Board, 2023).

Entre las principales directrices formuladas por estos organismos se destacan la necesidad de fortalecer la coordinación internacional, adoptar regulaciones proporcionales al riesgo, preservar la estabilidad financiera, supervisar adecuadamente los riesgos asociados a las *stablecoins*, reforzar la supervisión de los intermediarios relevantes y prevenir el arbitraje regulatorio entre distintas jurisdicciones. Estas recomendaciones permiten comprender el impacto sistémico que los activos virtuales pueden generar sobre el sistema financiero internacional.

Desde la auditoría forense, estas recomendaciones son relevantes porque permiten contextualizar los riesgos sistémicos y transfronterizos que pueden afectar operaciones investigadas.

4.6.6 IOSCO y protección de los mercados

La Organización Internacional de Comisiones de Valores (IOSCO) ha emitido recomendaciones para los mercados de criptoactivos y activos digitales, orientadas a proteger a los inversionistas, preservar la integridad del mercado y reducir riesgos de manipulación, conflictos de interés y custodia inadecuada. En 2023, IOSCO publicó sus recomendaciones de política para mercados de criptoactivos y activos digitales.

Estas recomendaciones resultan especialmente relevantes cuando los activos virtuales funcionan como instrumentos de inversión, *tokens* negociables o productos vinculados a mercados de capitales (International Organization of Securities Commissions [IOSCO], 2023).

Para el auditor forense, el marco desarrollado por IOSCO proporciona criterios útiles para evaluar posibles prácticas de manipulación de precios, conflictos de interés en las plataformas de negociación, riesgos asociados a la custodia de

activos virtuales, deficiencias en la segregación patrimonial y limitaciones en la transparencia de la información suministrada a los inversionistas. Estos aspectos resultan particularmente relevantes cuando los activos virtuales cumplen funciones de inversión o se negocian en mercados organizados.

4.6.7 Banco de Pagos Internacionales y Comité de Basilea

El Banco de Pagos InternacionaInternacionales (BIS) y el Comité de Basilea han desarrollado estándares prudenciales relacionados con la exposición de entidades bancarias a criptoactivos. Estos criterios buscan que los bancos mantengan niveles adecuados de capital, revelen sus exposiciones y gestionen los riesgos derivados de activos digitales (Basel Committee on Banking Supervision, 2022).

A partir de 2026, los estándares de divulgación aprobados por reguladores bancarios globales exigirán que los bancos publiquen información sobre sus exposiciones a criptoactivos, con el objetivo de fortalecer la disciplina de mercado y mejorar la disponibilidad de información.

Desde la auditoría forense, estas directrices permiten analizar la exposición institucional a criptoactivos, la suficiencia de revelaciones y la calidad de los controles internos vinculados a riesgos tecnológicos y financieros.

Bajo un enfoque de auditoría forense, estas directrices permiten ampliar el análisis más allá de cada transacción individual, considerando aspectos como las obligaciones de reporte fiscal, la cooperación internacional entre autoridades, la identificación de usuarios y beneficiarios finales, la trazabilidad de las operaciones, los riesgos asociados a la custodia de activos digitales, la exposición de las entidades financieras a criptoactivos y la participación de intermediarios registrados o no registrados. La integración de estos elementos fortalece la obtención de evidencia documental y tecnológica, especialmente en investigaciones con componentes transfronterizos.

Las iniciativas desarrolladas por la OCDE, el FMI, la FSB, IOSCO, el Banco de Pagos Internacionales y el Comité de Basilea evidencian una creciente convergencia internacional en torno a la regulación de los activos virtuales. Bajo un enfoque de auditoría forense, estos instrumentos proporcionan criterios útiles para evaluar la transparencia fiscal, la trazabilidad de las operaciones, la identificación de beneficiarios finales, la suficiencia de los controles internos y los riesgos asociados a transacciones transfronterizas. En consecuencia, el conocimiento de estas directrices permite fortalecer la obtención y valoración de evidencia en investigaciones relacionadas con criptoactivos.

4.6.8 Conclusiones

Las directrices emitidas por los organismos multilaterales complementan los estándares del GAFI al incorporar dimensiones tributarias, prudenciales y de estabilidad financiera. Si bien responden a ámbitos de actuación distintos, en conjunto ofrecen un marco de referencia que facilita la cooperación internacional y fortalece las prácticas de auditoría y control aplicables al ecosistema de los activos virtuales.

Tabla No. 9

Directrices de organismos multilaterales aplicables a activos virtuales

Organismo	Instrumento principal	Aplicación en auditoría forense
OCDE	CARF y CRS actualizado	Identificación de operaciones reportables e intercambio de información fiscal.
FMI / FSB	Hoja de ruta y recomendaciones de política sobre criptoactivos	Evaluación de riesgos macrofinancieros y transfronterizos.
IOSCO	Recomendaciones para mercados de criptoactivos	Análisis de integridad de mercado, custodia y protección del inversionista.
BIS / Comité de Basilea	Estándares prudenciales y revelaciones bancarias	Evaluación de exposición bancaria y suficiencia de controles.
G20	Coordinación internacional	Impulso político para la convergencia regulatoria global.

Nota: Elaboración propia con base en la OCDE (2022, 2023), el Fondo Monetario Internacional y el Financial Stability Board (2023), la International Organization of Securities Commissions (IOSCO, 2023) y el Basel Committee on Banking Supervision (2022).

4.7 Compliance y Debida Diligencia Digital

4.7.1 Introducción

La expansión del ecosistema de activos virtuales ha incrementado la necesidad de fortalecer los mecanismos de cumplimiento normativo (*Compliance*) y de debida diligencia digital, con el propósito de prevenir riesgos asociados al lavado de activos, el financiamiento del terrorismo, el fraude, la evasión fiscal y otros delitos económicos. La naturaleza descentralizada de la tecnología

blockchain, la rapidez de las transacciones y la posibilidad de operar a través de múltiples jurisdicciones exigen que las organizaciones implementen controles internos eficaces y procedimientos de gestión de riesgos acordes con los estándares internacionales.

En este contexto, el *Compliance* constituye un elemento esencial para garantizar el cumplimiento de las obligaciones legales, regulatorias y éticas aplicables a los proveedores de servicios de activos virtuales (PSAV), entidades financieras y demás organizaciones que intervienen en el ecosistema digital. Paralelamente, la debida diligencia digital incorpora herramientas tecnológicas que permiten identificar a los usuarios, verificar el origen de los fondos, monitorear operaciones y preservar evidencia digital, fortaleciendo la transparencia y la integridad de las operaciones.

Desde la perspectiva de la auditoría forense, estos mecanismos proporcionan información relevante para la evaluación de riesgos, la obtención de evidencia y la reconstrucción de operaciones relacionadas con activos virtuales.

4.7.2 Compliance en el ecosistema de activos virtuales

El *Compliance* puede definirse como el conjunto de políticas, procedimientos, controles y buenas prácticas implementados por una organización para asegurar el cumplimiento de la normativa vigente y reducir la exposición a riesgos legales, financieros, operacionales y reputacionales (FATF, 2023).

En el ámbito de los activos virtuales, un programa de cumplimiento efectivo debe contemplar la identificación y evaluación periódica de riesgos, políticas internas de prevención del lavado de activos y del financiamiento del terrorismo, una adecuada asignación de responsabilidades de supervisión, programas permanentes de capacitación, mecanismos de monitoreo continuo de operaciones, canales para el reporte de operaciones inusuales o sospechosas, procedimientos para la conservación segura de la información y la evidencia digital, así como revisiones periódicas destinadas a evaluar la eficacia de los controles internos implementados.

La efectividad de estos programas depende de la participación activa de la alta dirección y de la existencia de una cultura organizacional orientada al cumplimiento y la gestión de riesgos.

4.7.3 Debida diligencia del cliente (Know Your Customer – KYC)

La identificación adecuada del cliente constituye uno los pilares fundamentales del sistema de prevención del lavado de activos. El principio *Know Your Customer* (KYC) exige que las organizaciones conozcan razonablemente la identidad de sus clientes antes de establecer una relación comercial y durante toda su vigencia.

Los procedimientos de *Know Your Customer* (KYC) comprenden la identificación y verificación de la identidad del cliente, la obtención de información sobre la actividad económica desarrollada, la determinación del propósito de la relación comercial, la evaluación del perfil de riesgo y la actualización periódica de la información obtenida durante toda la relación comercial (FATF, 2023).

En el entorno digital, estos procedimientos pueden apoyarse en mecanismos de verificación electrónica de identidad, autenticación multifactor y validación documental mediante tecnologías especializadas, siempre respetando la normativa aplicable en materia de protección de datos personales.

4.7.4 Identificación del beneficiario final y Know Your Business (KYB)

Además de identificar a los clientes, los estándares internacionales exigen determinar quién ejerce el control efectivo sobre las personas jurídicas o estructuras legales involucradas en una operación.

El procedimiento denominado *Know Your Business* (KYB) complementa el KYC mediante la verificación de la existencia legal de la entidad, su estructura societaria, la identificación de sus representantes y del beneficiario final (FATF, 2023), así como la evaluación de su actividad económica.

La correcta identificación del beneficiario final resulta especialmente relevante en operaciones con activos virtuales, donde la utilización de estructuras societarias complejas o múltiples billeteras digitales puede dificultar la identificación de los verdaderos titulares de los activos.

4.7.5 Monitoreo de transacciones y Know Your Transaction (KYT)

El monitoreo continuo de operaciones constituye un componente esencial de los programas de cumplimiento.

En el ecosistema blockchain, este proceso ha evolucionado hacia el modelo *Know Your Transaction* (KYT), que utiliza herramientas tecnológicas para analizar en tiempo real el comportamiento de las transacciones y detectar operaciones que presenten características inusuales o de alto riesgo.

Entre los principales indicadores analizados mediante herramientas de *Know Your Transaction* (KYT) se encuentran el volumen y la frecuencia de las operaciones, la utilización de servicios de mezcla (*mixers*), las transacciones realizadas con billeteras previamente identificadas como riesgosas, los movimientos hacia jurisdicciones de alto riesgo, las operaciones fraccionadas y los patrones transaccionales atípicos que puedan evidenciar comportamientos incompatibles con el perfil del cliente (FATF, 2023).

El KYT permite complementar los procedimientos tradicionales de monitoreo y facilita la detección temprana de posibles actividades ilícitas.

4.7.6 Blockchain Analytics y trazabilidad digital

El desarrollo de herramientas de *Blockchain Analytics* ha transformado significativamente la forma en que se investigan las operaciones con activos virtuales.

Estas soluciones permiten analizar la información contenida en las cadenas de bloques para identificar relaciones entre direcciones, reconstruir flujos de transacciones, detectar patrones de comportamiento y asociar determinadas billeteras con actividades previamente identificadas por organismos de supervisión o autoridades judiciales.

Aunque la blockchain proporciona un registro inmutable de las operaciones, el análisis técnico continúa siendo indispensable para interpretar adecuadamente la información disponible y vincular las direcciones criptográficas con personas físicas o jurídicas cuando ello resulte legalmente posible.

4.7.7 Conservación de registros y evidencia digital

Los programas de cumplimiento deben garantizar la conservación íntegra, segura y accesible de la información relacionada con las operaciones realizadas.

La preservación de registros comprende la documentación utilizada para la identificación del cliente y del beneficiario final, los registros de transacciones, las comunicaciones relevantes, los soportes electrónicos, la evidencia criptográfica y los registros generados por los sistemas de auditoría informática.

Desde la auditoría forense, la adecuada conservación de esta información resulta esencial para mantener la cadena de custodia de la evidencia digital y garantizar su disponibilidad durante eventuales investigaciones administrativas o judiciales.

4.7.8 Implicancias para la auditoría forense

La evaluación del sistema de cumplimiento constituye una etapa esencial dentro de la auditoría forense de activos virtuales.

En consecuencia, el auditor deberá analizar la existencia y eficacia del programa de *Compliance*, la correcta aplicación de los procedimientos KYC, KYB y KYT, la identificación del beneficiario final, la documentación de las operaciones, los mecanismos de monitoreo implementados, la conservación de registros y evidencia digital, así como la efectividad de los controles internos relacionados con activos virtuales. La calidad de estos elementos influye directamente en la confiabilidad de la información financiera y en la posibilidad de reconstruir operaciones objeto de investigación.

4.7.9 Reflexiones finales

La consolidación de los programas de *Compliance* y de los procesos de debida diligencia digital constituye uno de los principales desafíos para las organizaciones que operan con activos virtuales. Más allá del cumplimiento de obligaciones regulatorias, estos sistemas representan herramientas de gestión que fortalecen la transparencia, reducen la exposición a riesgos y mejoran la calidad de la información disponible para la toma de decisiones.

Desde la auditoría forense, el análisis de los mecanismos de cumplimiento, de la identificación del cliente y del beneficiario final, del monitoreo de transacciones y de la preservación de la evidencia digital permite comprender con mayor precisión la dinámica de las operaciones investigadas. En un entorno caracterizado por la innovación tecnológica y la evolución constante de los riesgos, el profesional debe combinar el conocimiento de los estándares internacionales con competencias técnicas especializadas, manteniendo un enfoque crítico que contribuya a la confiabilidad de sus conclusiones y al fortalecimiento de la integridad del sistema financiero.

Tabla No. 10

Principales componentes del Compliance y la debida diligencia digital aplicables a los activos virtuales

Componente	Objetivo	Aplicación en auditoría forense
Compliance	Cumplimiento normativo y gestión de riesgos	Evaluación de políticas, controles internos y gobierno corporativo.
KYC (Know Your Customer)	Identificación y verificación del cliente	Validación de identidad y perfil de riesgo.
KYB (Know Your Business)	Identificación de personas jurídicas y beneficiario final	Verificación de estructuras societarias y control efectivo.
KYT (Know Your Transaction)	Monitoreo de transacciones	Detección de operaciones inusuales y patrones de riesgo.
Blockchain Analytics	Análisis de transacciones en blockchain	Reconstrucción de flujos, trazabilidad y obtención de evidencia digital.
Conservación de registros	Preservación de documentación y evidencia	Mantenimiento de la cadena de custodia y soporte probatorio.

Fuente: Elaboración propia con base en las Recomendaciones del GAFI (FATF, 2023), la Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (FATF, 2023) y el Crypto-Asset Reporting Framework (OECD, 2022)s.

5 TRATAMIENTO CONTABLE Y TRIBUTARIO DE CRIPTOACTIVOS

5.1 Reconocimiento contable de activos virtuales

La expansión de los activos virtuales y de las tecnologías de registro distribuido ha planteado nuevos desafíos para la contabilidad financiera, debido a que las características económicas de estos activos no siempre coinciden con las categorías tradicionales previstas en las normas contables. Criptomonedas, *tokens*, *stablecoins*, *tokens* no fungibles (*non-fungible tokens* – NFT), activos tokenizados y otras representaciones digitales pueden utilizar tecnologías similares, pero otorgar derechos económicos sustancialmente diferentes. Por consiguiente, desde una perspectiva contable, la tecnología utilizada para representar o transferir un activo no determina, por sí misma, su clasificación.

El Grupo de Acción Financiera define el activo virtual como una representación digital de valor que puede negociarse o transferirse digitalmente y utilizarse para fines de pago o inversión, excluyendo determinadas representaciones digitalizadas de monedas fiduciarias, valores y otros activos financieros que ya se encuentran comprendidos en categorías regulatorias específicas (Financial Action Task Force [FATF], 2023). Esta definición tiene principalmente una finalidad regulatoria vinculada con la prevención del lavado de activos y el financiamiento del terrorismo; por ello, no constituye por sí sola una definición contable.

De forma más amplia, el Marco de Reporte de Criptoactivos (*Crypto-Asset Reporting Framework* – CARF) desarrollado por la Organización para la Cooperación y el Desarrollo Económicos comprende como criptoactivos aquellas representaciones digitales de valor cuya creación, tenencia o transferencia se fundamenta en tecnologías de registro distribuido protegidas criptográficamente o tecnologías similares. Dentro de esta perspectiva pueden encontrarse *stablecoins*, determinados derivados representados mediante criptoactivos y ciertos NFT (Organización para la Cooperación y el Desarrollo Económicos [OCDE], 2023).

Sin embargo, bajo las Normas Internacionales de Información Financiera (NIIF) no existe una única categoría contable denominada “activo virtual” o

"criptoactivo" que resulte aplicable indistintamente a todas estas representaciones digitales. La identificación y reconocimiento contable debe efectuarse atendiendo a las características económicas del activo, los derechos que incorpora, las circunstancias de su tenencia y el modelo de negocio de la entidad. En consecuencia, dos *tokens* tecnológicamente semejantes pueden requerir tratamientos contables distintos cuando los derechos económicos que representan son diferentes.

5.1.1 El reconocimiento desde el Marco Conceptual para la Información Financiera

El punto de partida para determinar si un activo virtual debe ser reconocido contablemente se encuentra en el Marco Conceptual para la Información Financiera. Conforme a este marco, un activo constituye un recurso económico presente controlado por la entidad como resultado de sucesos pasados, mientras que un recurso económico corresponde a un derecho que posee el potencial de producir beneficios económicos (IFRS Foundation, 2018).

Esta definición permite identificar tres elementos fundamentales aplicables a los activos virtuales: existencia de un recurso económico presente, control por parte de la entidad y origen en un suceso pasado. Por tanto, la simple existencia de una dirección blockchain, un registro digital o una determinada cantidad de *tokens* asociada a una *wallet* no resulta suficiente para concluir automáticamente que existe un activo reconocido contablemente.

El derecho debe tener el potencial de generar beneficios económicos para la entidad. El Marco Conceptual reconoce que dichos beneficios pueden materializarse, entre otras formas, mediante la recepción de flujos de efectivo u otros recursos económicos, el intercambio del recurso con terceros, su utilización para producir bienes o prestar servicios, su venta o su utilización para extinguir obligaciones (IFRS Foundation, 2018).

En el ámbito de los criptoactivos, dicho potencial económico puede manifestarse mediante su venta en mercados, su intercambio por otros activos, su utilización como medio de pago cuando sea aceptado, la obtención de determinados derechos contractuales o económicos o, dependiendo de sus características, su utilización dentro de determinados ecosistemas digitales. En consecuencia, el reconocimiento contable debe atender a la capacidad económica del recurso y no exclusivamente a su denominación comercial.

Adicionalmente, el reconocimiento implica incorporar en los estados financieros un elemento que cumple la definición correspondiente, representándolo mediante una descripción y un importe monetario. Este proceso requiere con-

siderar si el reconocimiento proporciona información relevante y una representación fiel del fenómeno económico que se pretende reflejar (IFRS Foundation, 2018).

5.1.2 El control como elemento esencial del reconocimiento

Uno de los aspectos más relevantes en el reconocimiento contable de activos virtuales es determinar si la entidad controla efectivamente el recurso económico.

El Marco Conceptual vincula el control con la capacidad de dirigir el uso de un recurso económico y obtener los beneficios económicos derivados de él. En el caso particular de los activos intangibles, la NIC 38 desarrolla esta noción al considerar que existe control cuando la entidad posee el poder de obtener los beneficios económicos futuros procedentes del recurso y restringir el acceso de terceros a dichos beneficios (IFRS Foundation, 2024).

La aplicación de este concepto a los criptoactivos reviste particular complejidad debido a la existencia de diferentes modalidades de custodia. En una *wallet* de autocustodia, por ejemplo, la capacidad de utilizar las claves criptográficas necesarias para disponer del activo constituye un elemento técnico relevante para evaluar el control. Sin embargo, desde el punto de vista contable y forense, la posesión o conocimiento de una clave privada no debe interpretarse aisladamente como prueba concluyente de propiedad económica. Debe determinarse quién posee realmente la facultad de disponer del activo, quién asume los riesgos asociados y quién tiene derecho a obtener los beneficios económicos derivados de su utilización o transferencia.

Esta distinción adquiere mayor relevancia cuando los criptoactivos se encuentran depositados o custodiados en un *exchange* centralizado, una plataforma de negociación, una entidad financiera o un custodio especializado. En estos supuestos debe analizarse la relación contractual existente entre el titular y el custodio, debido a que el registro mostrado en una plataforma puede representar un derecho contractual frente al intermediario y no necesariamente un control directo sobre unidades concretas registradas en blockchain.

Desde una perspectiva de auditoría forense, por consiguiente, la constatación del saldo mostrado en una plataforma digital no debería considerarse evidencia suficiente de reconocimiento. Resulta necesario correlacionar la información del sistema con contratos de custodia, registros blockchain, direcciones de *wallets*, documentación KYC, movimientos de ingreso y salida, registros

internos, información proporcionada por *exchanges* y demás elementos que permitan establecer la titularidad económica y capacidad real de disposición.

5.1.3 Identificabilidad y separabilidad del activo virtual

Cuando un criptoactivo queda comprendido en la NIC 38 *Activos intangibles*, debe cumplir la definición de activo intangible, es decir, ser un activo identificable, de carácter no monetario y sin apariencia física. La identificabilidad se presenta cuando el recurso es separable o surge de derechos contractuales u otros derechos legales (IFRS Foundation, 2024).

La separabilidad constituye una característica particularmente relevante de las criptomonedas transferibles. Un criptoactivo susceptible de ser vendido o transferido independientemente del resto de los activos de la entidad satisface, en principio, esta característica. Precisamente, el *IFRS Interpretations Committee* determinó en 2019 que las criptomonedas comprendidas dentro del supuesto analizado satisfacen la definición de activo intangible porque pueden separarse de su titular y venderse o transferirse individualmente, y porque no otorgan un derecho a recibir un número fijo o determinable de unidades monetarias (IFRS Interpretations Committee, 2019).

Debe advertirse, sin embargo, que esta conclusión no fue formulada para la totalidad de los criptoactivos existentes. La decisión del Comité se circunscribió a una categoría específica de criptomonedas caracterizadas por encontrarse registradas en un libro mayor distribuido protegido mediante criptografía, no haber sido emitidas por una autoridad jurisdiccional u otra parte y no generar un contrato entre su titular y otra parte (IFRS Interpretations Committee, 2019).

Esta precisión resulta fundamental porque impide extender automáticamente la decisión sobre Bitcoin u otras criptomonedas descentralizadas a *stablecoins* respaldadas por un emisor, *security tokens*, tokens representativos de deuda, activos tokenizados o instrumentos que incorporan derechos contractuales.

5.1.4 Diferenciación entre criptomoneda, efectivo y activo financiero

Otro aspecto esencial consiste en determinar si determinadas criptomonedas pueden ser reconocidas como efectivo.

El *IFRS Interpretations Committee* analizó esta cuestión considerando que el efectivo constituye el medio de intercambio que sirve de base para la medición y reconocimiento de las operaciones. Aunque determinadas criptomonedas pueden emplearse para adquirir bienes o servicios, el Comité concluyó que las criptomonedas comprendidas en su análisis no poseían las características necesarias para ser consideradas efectivo, debido a que no eran utilizadas como medio de intercambio y unidad monetaria de fijación de precios en una magnitud suficiente para constituir la base general de reconocimiento de las transacciones (IFRS Interpretations Committee, 2019).

De igual forma, estas criptomonedas no fueron consideradas activos financieros. La NIC 32 comprende dentro del concepto de activo financiero, entre otros supuestos, el efectivo, instrumentos de patrimonio de otras entidades y derechos contractuales a recibir efectivo u otro activo financiero. Una criptomoneda descentralizada que no represente efectivo, no constituya un instrumento de patrimonio de otra entidad y no origine un derecho contractual frente a una contraparte no satisface dichas condiciones (IFRS Interpretations Committee, 2019).

Esta conclusión resulta especialmente importante para evitar uno de los errores más frecuentes en la práctica contable: registrar automáticamente toda criptomoneda dentro de "efectivo y equivalentes de efectivo", "inversiones financieras" o "valores negociables" únicamente porque posee liquidez o puede convertirse rápidamente en moneda fiduciaria.

La elevada liquidez de un activo no modifica por sí misma su naturaleza contable. Una criptomoneda puede disponer de mercados activos y ser fácilmente convertida en dólares, euros u otra moneda fiduciaria sin que ello la convierta necesariamente en efectivo o en un instrumento financiero bajo las NIIF.

5.1.5 Reconocimiento como activo intangible bajo la NIC 38

Para las criptomonedas comprendidas en el supuesto analizado por el *IFRS Interpretations Committee*, el tratamiento residual generalmente aplicable es la NIC 38 *Activos intangibles*, salvo que correspondan al ámbito de la NIC 2 *Inventarios*.

El Comité concluyó que una tenencia de criptomonedas de esas características satisface la definición de activo intangible porque es identificable, carece de sustancia física y es de naturaleza no monetaria. Además, puede separarse del titular y transferirse individualmente, sin conferir un derecho contractual a

recibir una cantidad fija o determinable de moneda (IFRS Interpretations Committee, 2019).

En términos generales, la NIC 38 exige que un recurso satisfaga tanto la definición de activo intangible como los criterios previstos para su reconocimiento. La norma contempla que los beneficios económicos futuros asociados al activo sean probables y que su costo pueda ser medido de manera fiable. En el caso de activos intangibles adquiridos separadamente, la propia contraprestación pagada normalmente incorpora las expectativas relacionadas con los beneficios económicos, mientras que el costo suele ser susceptible de medición fiable (IFRS Foundation, 2024).

Consecuentemente, cuando una entidad adquiere directamente una criptomoneda susceptible de aplicación de la NIC 38, existe normalmente un suceso pasado claramente identificable la adquisición y una contraprestación que puede constituir la base para establecer su reconocimiento inicial. Los aspectos relacionados con la determinación del importe inicial, costos de transacción, valoración posterior, deterioro, vida útil y posible aplicación del modelo de revaluación corresponden fundamentalmente al apartado

5.1.6 Amortización de criptomonedas clasificadas como activos intangibles

La aplicación de la NIC 38 exige analizar si los activos intangibles reconocidos tienen una vida útil finita o indefinida.

La norma establece que un activo intangible con vida útil finita debe ser amortizado de forma sistemática a lo largo de su vida útil estimada, mientras que un activo con vida útil indefinida no se amortiza, pero debe someterse anualmente a pruebas de deterioro, o con mayor frecuencia si existen indicios de pérdida de valor (IFRS Foundation, 2026, NIC 38, párrs. 88-107).

En el caso particular de las criptomonedas descentralizadas (como Bitcoin u otras tenencias similares que no otorgan derechos de duración limitada ni derechos contractuales extintos), la evaluación de la vida útil suele concluir que no existe un límite previsible para el período durante el cual el activo se espera que genere entradas de netos flujos de efectivo para la entidad. Por consiguiente, bajo las condiciones examinadas habitualmente, estas criptomonedas se clasifican con frecuencia como activos intangibles de vida útil indefinida.

Esta clasificación implica que:

No se practica amortización periódica, evitando imputar un gasto sistemático por el uso o el paso del tiempo.

Se debe realizar una prueba de deterioro anual (o cuando existan indicios de desvalorización) comparando el importe en libros del criptoactivo con su importe recuperable (definido como el mayor entre su valor razonable menos los costos de disposición y su valor en uso).

Desde la perspectiva de la auditoría forense, cuando una entidad amortiza criptomonedas de vida útil indefinida, o bien omite realizar las pruebas de deterioro requeridas ante caídas drásticas de precios en el mercado, se generan distorsiones probatorias y contables que deben ser documentadas y evaluadas en el peritaje financiero.

5.1.7 Medición inicial y posterior de criptoactivos clasificados como inventarios (NIC 2)

Cuando las criptomonedas o activos virtuales son mantenidos para su venta en el curso ordinario de las actividades de la entidad o cuando la organización opera bajo el modelo de *broker-trader*, la normativa aplicable es la NIC 2 Inventarios (IFRS International Accounting Standards Board [IASB], 2026).

1. Medición Inicial

Los inventarios de criptoactivos se miden inicialmente al **costo**, el cual comprende todos los costos de adquisición, costos de transformación y otros costos incurridos para poner los activos en su ubicación y condición actuales (IASB, 2026, NIC 2, párr. 10). En el caso de comercializadores o intermediarios financieros (*broker-traders*), los costos directos de transacción, comisiones de negociación y tarifas de red estrictamente necesarias se incorporan al costo inicial.

2. Medición Posterior

Conforme al párrafo 9 de la NIC 2, los inventarios se miden al menor entre el costo y el valor neto realizable (VNR) (IASB, 2026, NIC 2, párr. 9).

Si el precio de mercado de la criptomoneda desciende por debajo de su costo de adquisición, la entidad debe reconocer una corrección de valor (deterioro de inventario) directamente en los resultados del período.

Tratándose específicamente de broker-traders, la norma contempla un tratamiento diferenciado y ampliamente utilizado en la práctica de los mercados de materias primas e intermediación digital: los inventarios se miden al valor razonable menos los costos de venta, reconociendo los cambios en dicho valor razonable directamente en los resultados del período en que se producen (IASB, 2026, NIC 2, párr. 3).

5.1.8 Medición de criptoactivos que incorporan derechos contractuales (NIIF 9)

Cuando el activo digital califica como un instrumento financiero bajo la NIC 32 (por ejemplo, *security tokens*, tokens representativos de deuda o *stablecoins* con derecho contractual exigible de reembolso frente a un emisor solvente), su medición se rige por la NIIF 9 Instrumentos Financieros (IFRS Foundation, 2026, NIIF 9).

La medición bajo la NIIF 9 depende de dos variables fundamentales:

- El modelo de negocio de la entidad para gestionar los activos financieros.
- Las características de los flujos de efectivo contractuales del activo digital (prueba SPPI: *Solely Payments of Principal and Interest*).

Conforme a estos criterios, los criptoactivos financieros pueden medirse a:

- Costo amortizado: Cuando el modelo de negocio tiene como objetivo mantener el activo para recolectar flujos de efectivo contractuales y los flujos corresponden únicamente a pagos de principal e intereses.
- Valor razonable con cambios en otro resultado integral (VRCORI): Cuando el modelo de negocio busca tanto la recolección de flujos contractuales como la venta del activo.
- Valor razonable con cambios en resultados (VRCR): Es la categoría residual más frecuente para activos digitales negociables o carteras gestionadas bajo modelo de negociación (*trading*), donde el activo no cumple los requisitos de costo amortizado ni de VRCORI.

5.1.9 Relevancia de la jerarquía del valor razonable (NIIF 13)

Independientemente de que un activo virtual se mida a valor razonable por aplicación de la NIC 38 (modelo de revaluación), de la NIC 2 (régimen de *broker-traders*) o de la NIIF 9, la determinación de dicho valor razonable debe ajustarse estrictamente a los parámetros establecidos en la NIIF 13 Medición del Valor Razonable (IFRS Foundation, 2026, NIIF 13).

La NIIF 13 define el valor razonable como el precio que se recibiría por vender un activo o se pagaría por transferir un pasivo en una transacción ordenada entre participantes del mercado en la fecha de medición (precio de salida). Para garantizar la fiabilidad de la valoración, la norma establece una jerarquía de valor razonable basada en tres niveles de datos de entrada (*inputs*):

Nivel 1: Precios cotizados (no ajustados) en mercados activos para activos idénticos a los que la entidad puede acceder en la fecha de medición. En el

ecosistema de criptoactivos, esto corresponde a cotizaciones públicas en *exchanges* altamente líquidos y profundos.

Nivel 2: Datos de entrada diferentes de los precios cotizados incluidos en el Nivel 1 que sean observables para el activo, directa o indirectamente (por ejemplo, precios cotizados para activos similares en mercados activos o precios derivados de modelos estadísticos con variables observables).

Nivel 3: Datos de entrada no observables para el activo (utilizados cuando el mercado no es activo o cuando se trata de activos ilíquidos, NFT exclusivos o *tokens* sin cotización pública contrastable).

Desafíos en la valoración forense de criptoactivos

En la práctica pericial y contable, la valoración de criptoactivos bajo la NIIF 13 presenta desafíos significativos que el auditor forense debe examinar con rigor:

Fragmentación de precios entre *exchanges*: Distintas plataformas centralizadas o descentralizadas pueden registrar precios diferentes para un mismo token en un instante determinado. La entidad debe definir y documentar cuál es su mercado principal (o el mercado más ventajoso en ausencia de un mercado principal).

Volatilidad y ventanas temporales: La fluctuación continua (24/7) exige precisar la hora exacta de la medición (asociada al *timestamp* de la transacción o al corte contable) para evitar distorsiones materiales en los estados financieros.

Liquidez y profundidad: La existencia de un precio visible en pantalla no garantiza que el volumen operado sea suficiente para liquidar la posición completa sin generar un impacto significativo en el precio (riesgo de liquidez y descuento por profundidad de mercado).

5.1.10 Matriz de medición y valoración aplicable a activos virtuales

Naturaleza del activo digital	Norma NIIF aplicable	Base de medición inicial	Bases de medición posterior permitidas / requeridas
Criptomoneda descentralizada (inversión)	NIC 38 (Activos Intangibles)	Costo (precio de adquisición + costos directamente atribuibles)	Modelo del costo (costo menos amortización y deterioro) o Modelo de revaluación (valor razonable con mercado activo).

Naturaleza del activo digital	Norma NIIF aplicable	Base de medición inicial	Bases de medición posterior permitidas / requeridas
Criptomoneda / Token mantenido para venta (ordinario)	NIC 2 (Inventarios)	Costo de adquisición e incorporación de costos directos	Menor entre el costo y el valor neto realizable (VNR).
Inventario de criptoactivos (*Broker-Traders*)	NIC 2 (Inventarios - Excepción)	Costo de adquisición	Valor razonable menos los costos de venta (cambios en resultados).
Token con derechos contractuales de crédito o pago	NIIF 9 (Instrumentos Financieros)	Valor razonable más costos de transacción (salvo VRCR)	Costo amortizado, VRCORI o VRCR, según modelo de negocio y prueba SPPI.
Stablecoin con derecho exigible de reembolso	NIIF 9 o NIC 32	Valor razonable / Importe nominal exigible	Medición financiera correspondiente según clasificación contractual.
Utility Token / NFT / RWA	NIC 8 (Juicio Profesional) / NIIF específica	Costo inicial según sustancia económica	Evaluación individual basada en la naturaleza del recurso subyacente.

Nota: Elaboración propia con base en el Marco Conceptual para la Información Financiera (IFRS Foundation, 2018), NIC 2, NIC 38, NIIF 9 y NIIF 13 (IFRS Foundation, 2026; IASB, 2026).

5.1.11 Implicancias de la medición en la auditoría forense

Desde la óptica de la auditoría forense, la verificación de la medición y valoración de los activos virtuales cumple un rol determinante para detectar anomalías financieras, ocultación de activos, sobrevaloración patrimonial o manipulación de resultados.

Los procedimientos periciales orientados a evaluar la medición contable deben contemplar:

- **Validación de fuentes de cotización:** Comprobar que los precios unitarios utilizados para valorar el inventario o la inversión al cierre del período provengan de mercados activos reconocidos y coherentes con la política contable de la entidad.
- **Correlación de saldos on-chain con registros contables:** Cruzar los importes monetarios expresados en los estados financieros con las tenencias reales identificadas en las direcciones de *wallets* controladas.
- **Revisión de deterioros no reconocidos:** Identificar si la entidad ha omitido registrar pérdidas por deterioro o correcciones de valor ante caídas sostenidas en las cotizaciones de los criptoactivos mantenidos.

- **Análisis de transacciones complejas:** Examinar la razonabilidad del valor razonable asignado en operaciones de permuta (*crypto-to-crypto*) o en la recepción de activos mediante minería, *staking* o *airdrops*, donde la ausencia de contraprestación en moneda fiduciaria dificulta la determinación objetiva del costo inicial.

La integración rigurosa entre los criterios de medición de las NIIF y la evidencia digital obtenida mediante análisis forense constituye la base indispensable para emitir dictámenes periciales sólidos y confiables en investigaciones sobre delitos económicos y financieros vinculados a ecosistemas cripto.

5.2 Medición y valoración

La medición constituye una etapa esencial del tratamiento contable de los activos virtuales, debido a que permite asignar una expresión monetaria a los recursos económicos reconocidos en los estados financieros. En el caso de los criptoactivos, esta función adquiere una complejidad particular debido a su volatilidad, la existencia de múltiples plataformas de negociación, la negociación continua durante las veinticuatro horas del día, las diferencias de liquidez entre mercados y la diversidad económica de los instrumentos comprendidos bajo la denominación general de activos virtuales.

Desde la perspectiva de las Normas Internacionales de Información Financiera (NIIF), no existe una única base de medición aplicable a todos los criptoactivos. Como se desarrolló en el apartado anterior, la norma que determina su medición depende de su naturaleza económica y de la finalidad para la cual son mantenidos. Para las criptomonedas comprendidas en la decisión del IFRS Interpretations Committee de junio de 2019, corresponde aplicar la **NIC 2 Inventarios** cuando son mantenidas para su venta en el curso ordinario del negocio y, en los demás casos comprendidos en dicha decisión, la **NIC 38 Activos Intangibles**. Los criptoactivos que incorporen derechos contractuales y satisfagan la definición de activo financiero pueden, en cambio, encontrarse dentro del ámbito de la **NIIF 9 Instrumentos Financieros** (IFRS Interpretations Committee, 2019; IFRS Foundation, 2026).

En consecuencia, la valoración de un activo virtual no debe comenzar seleccionando una cotización disponible en una plataforma digital, sino determinando previamente **qué activo se está midiendo, bajo qué norma contable se encuentra clasificado, cuál es la unidad de cuenta, cuál es la base de medición aplicable y qué mercado o fuente de información resulta pertinente**.

5.2.1 Bases de medición aplicables a los activos virtuales

El Marco Conceptual para la Información Financiera distingue diferentes bases de medición y reconoce que la selección de una de ellas debe contribuir a producir información relevante y una representación fiel. Entre las principales bases se encuentran el costo histórico y las mediciones basadas en valores corrientes, dentro de las cuales se encuentra el valor razonable (IFRS Foundation, 2018).

Esta diferenciación resulta especialmente importante para los criptoactivos porque su **precio de mercado** no necesariamente coincide con su **importe en libros**. Una criptomoneda puede cotizar diariamente en un mercado por un importe considerablemente superior al costo pagado por la entidad, pero si la política contable aplicable exige mantenerla bajo el modelo del costo, la variación positiva de su precio no puede reconocerse automáticamente como ganancia.

Debe distinguirse, por tanto, entre los siguientes conceptos:

Concepto	Contenido
Costo	Importe inicialmente atribuido al activo de acuerdo con la norma aplicable.
Importe en libros	Valor por el cual el activo figura en el estado de situación financiera después de los ajustes requeridos.
Valor razonable	Precio que se recibiría por vender un activo en una transacción ordenada entre participantes del mercado en la fecha de medición.
Valor neto realizable	Precio estimado de venta en el curso ordinario de las operaciones menos los costos estimados necesarios para realizar la venta.
Importe recuperable	Mayor entre el valor razonable menos los costos de disposición y el valor en uso, dentro del ámbito de la NIC 36.

La correcta utilización de estos conceptos resulta indispensable debido a que no son intercambiables. Particularmente, **valor razonable y valor neto realizable representan bases distintas**: el primero utiliza una perspectiva de participantes del mercado, mientras que el segundo corresponde a una medición específica de la entidad para los inventarios (IFRS Foundation, 2026, NIIF 13 y NIC 2).

5.2.2 Medición inicial de criptomonedas clasificadas como activos intangibles

Cuando una tenencia de criptomonedas se encuentra dentro del ámbito de la NIC 38, la medición inicial se realiza **al costo**. Conforme al párrafo 24 de dicha norma, un activo intangible debe medirse inicialmente por su costo (IFRS Foundation, 2026, NIC 38, párr. 24). La normativa establece además que, tratándose de activos intangibles adquiridos separadamente, el costo comprende el precio de adquisición y aquellos desembolsos directamente atribuibles a preparar el activo para el uso previsto (IFRS Foundation, 2026, NIC 38, párrs. 27-30).

En una adquisición ordinaria de criptomonedas, el punto de partida será, por tanto, la contraprestación entregada para obtener el activo. Si una entidad adquiere 10 unidades de un determinado criptoactivo a US$ 5,000 cada una, la contraprestación básica asciende a US$ 50,000. Posteriormente deberá analizarse el tratamiento de los desembolsos directamente asociados con esa adquisición.

En operaciones mediante exchanges pueden existir **comisiones de negociación, tarifas de intermediación y costos propios de la red blockchain**. La incorporación de dichos desembolsos al costo deberá evaluarse de conformidad con los requisitos de la NIC 38 y la sustancia específica de la transacción. No resulta técnicamente correcto afirmar que toda comisión o *gas fee* se capitaliza automáticamente. Debe establecerse si constituye un costo directamente atribuible a la adquisición y colocación del activo en las condiciones necesarias para su utilización prevista.

Por consiguiente, la entidad deberá adoptar una política contable consistente que identifique:

Precio de adquisición + costos directamente atribuibles = costo inicial del criptoactivo, sujeto a que cada componente satisfaga los requisitos de la norma correspondiente.

Desde una perspectiva forense, esta evaluación implica contrastar el importe registrado contablemente con la orden ejecutada en el exchange, el comprobante de adquisición, la transferencia de fondos, las comisiones cargadas, el identificador de la transacción —*transaction hash* o *TxID*— y la recepción efectiva de los criptoactivos en la cuenta o wallet controlada por la entidad.

5.2.3 Determinación del costo cuando la adquisición se realiza con otro criptoactivo

Una situación frecuente en los ecosistemas digitales consiste en adquirir un criptoactivo entregando otro criptoactivo como contraprestación. Por ejemplo:

BTC → ETH

ETH → token

stablecoin → criptoactivo

En estos casos no existe necesariamente un desembolso directo en moneda fiduciaria. Por ello, debe evaluarse la norma aplicable a la permuta o intercambio de activos.

La NIC 38 contempla que un activo intangible adquirido mediante intercambio por otro activo monetario o no monetario se mida generalmente por su **valor razonable**, salvo determinadas excepciones, entre ellas cuando la transacción carezca de carácter comercial o cuando ni el valor razonable del activo recibido ni el del activo entregado pueda medirse de manera fiable (IFRS Foundation, 2026, NIC 38).

Esta situación reviste especial importancia para operaciones cripto-a-cripto porque la ausencia de dinero fiduciario **no significa que la operación carezca de valor económico ni que pueda omitirse su reconocimiento**.

Desde una perspectiva contable y pericial deberán identificarse, como mínimo:

- activo entregado;
- cantidad transferida;
- activo recibido;
- cantidad recibida;
- fecha y hora de la transacción;
- mercado pertinente;
- valor razonable utilizado;
- costos de la operación;
- diferencia entre el importe en libros del activo entregado y la contraprestación correspondiente;
- evidencia blockchain de la operación.

La trazabilidad entre ambos lados de la transacción constituye un elemento esencial para evitar que intercambios sucesivos entre criptoactivos sean erróneamente interpretados como simples transferencias internas.

5.2.4 Medición posterior bajo la NIC 38

Después del reconocimiento inicial, la NIC 38 permite optar, como política contable, entre el **modelo del costo** y el **modelo de revaluación**, sujeto a las condiciones establecidas por la propia norma. Si se utiliza el modelo de revaluación, este debe aplicarse a todos los activos pertenecientes a la misma clase, salvo aquellos respecto de los cuales no exista un mercado activo (IFRS Foundation, 2026, NIC 38, párrs. 72-75).

Esta elección produce consecuencias sustancialmente diferentes en el tratamiento de las variaciones de precio de los criptoactivos.

a) Modelo del costo

Bajo el modelo del costo, el activo intangible se presenta por:

Costo inicial
(–) amortización acumulada, cuando corresponda
(–) pérdidas acumuladas por deterioro
= importe en libros

La NIC 38 establece que, después del reconocimiento inicial, el activo contabilizado bajo este modelo debe mantenerse al costo menos la amortización acumulada y las pérdidas acumuladas por deterioro (IFRS Foundation, 2026, NIC 38, párr. 74).

Supóngase que una entidad adquirió Bitcoin por un costo de **US$ 40,000** y que al cierre su precio observable asciende a **US$ 65,000**. Si la entidad utiliza el modelo del costo, el incremento de US$ 25,000 **no se reconoce automáticamente como una ganancia**, aun cuando sea posible observar dicho precio en el mercado.

Esta característica constituye una de las principales diferencias entre el importe contable y el valor económico observable de determinadas criptomonedas.

En sentido contrario, una reducción importante en su valor puede requerir la aplicación de la NIC 36 cuando existan indicios de deterioro o cuando corresponda efectuar una prueba periódica obligatoria.

b) Modelo de revaluación

La NIC 38 permite alternativamente el modelo de revaluación. Bajo este modelo, después del reconocimiento inicial al costo, el activo se presenta a su valor razonable en la fecha de revaluación, menos cualquier amortización acumulada y pérdida por deterioro posterior. Sin embargo, existe una restricción fundamental: **el valor razonable debe poder determinarse por referencia a un mercado activo** (IFRS Foundation, 2026, NIC 38, párr. 75).

Esta condición adquiere particular relevancia para las criptomonedas.

La existencia de una cotización publicada en internet **no acredita automáticamente la existencia de un mercado activo a efectos de la NIC 38**. Debe

evaluarse si las transacciones del activo ocurren con suficiente frecuencia y volumen para proporcionar información de precios de manera continua.

Aunque la NIC 38 señala que los mercados activos son poco frecuentes para muchos activos intangibles tradicionales, determinados criptoactivos de elevada negociación pueden requerir un análisis específico de sus circunstancias de mercado. La existencia de múltiples exchanges, segmentos de mercado y pares de negociación hace necesario documentar cuidadosamente la conclusión alcanzada (IFRS Foundation, 2026, NIC 38; IFRS Foundation, 2026, NIIF 13).

5.2.5 Efectos contables de la revaluación

Cuando se cumplen las condiciones para aplicar el modelo de revaluación, los incrementos y disminuciones no reciben necesariamente el mismo tratamiento que las variaciones de instrumentos financieros medidos a valor razonable con cambios en resultados.

De acuerdo con la NIC 38, si el importe en libros aumenta como consecuencia de una revaluación, dicho incremento se reconoce generalmente en **otro resultado integral** y se acumula en el patrimonio como superávit de revaluación. No obstante, el incremento se reconocerá en resultados hasta el importe necesario para revertir una disminución previa del mismo activo que hubiese sido reconocida en resultados (IFRS Foundation, 2026, NIC 38, párr. 85).

Cuando la revaluación produce una disminución del importe en libros, esta se reconoce generalmente en resultados. Sin embargo, cuando existe un saldo acreedor previo en el superávit de revaluación correspondiente al mismo activo, la disminución se reconoce en otro resultado integral hasta agotar dicho saldo (IFRS Foundation, 2026, NIC 38, párr. 86).

Este tratamiento puede representarse de manera simplificada:

Situación	Tratamiento principal
Incremento de valor sin disminución anterior reconocida en resultados	Otro resultado integral / superávit de revaluación
Incremento que revierte una disminución anterior reconocida en resultados	Resultados, hasta el límite de la reversión
Disminución sin superávit previo	Resultados
Disminución existiendo superávit de revaluación del mismo activo	Otro resultado integral hasta el saldo disponible

Por tanto, la aplicación del modelo de revaluación no equivale a reconocer diariamente en resultados todas las fluctuaciones del precio de mercado de una criptomoneda.

5.2.6 Amortización de criptomonedas clasificadas como activos intangibles

La aplicación de la NIC 38 exige analizar si los activos intangibles reconocidos tienen una vida útil finita o indefinida.

La norma establece que un activo intangible con vida útil finita debe ser amortizado de forma sistemática a lo largo de su vida útil estimada, mientras que un activo con vida útil indefinida no se amortiza, pero debe someterse anualmente a pruebas de deterioro, o con mayor frecuencia si existen indicios de pérdida de valor (IFRS Foundation, 2026, NIC 38, párrs. 88-107).

En el caso particular de las criptomonedas descentralizadas (como Bitcoin u otras tenencias similares que no otorgan derechos de duración limitada ni derechos contractuales extintos), la evaluación de la vida útil suele concluir que no existe un límite previsible para el período durante el cual el activo se espera que genere entradas de netos flujos de efectivo para la entidad. Por consiguiente, bajo las condiciones examinadas habitualmente, estas criptomonedas se clasifican con frecuencia como activos intangibles de vida útil indefinida.

Esta clasificación implica que:

No se practica amortización periódica, evitando imputar un gasto sistemático por el uso o el paso del tiempo.

Se debe realizar una prueba de deterioro anual (o cuando existan indicios de desvalorización) comparando el importe en libros del criptoactivo con su importe recuperable (definido como el mayor entre su valor razonable menos los costos de disposición y su valor en uso).

Desde la perspectiva de la auditoría forense, cuando una entidad amortiza criptomonedas de vida útil indefinida, o bien omite realizar las pruebas de deterioro requeridas ante caídas drásticas de precios en el mercado, se generan distorsiones probatorias y contables que deben ser documentadas y evaluadas en el peritaje financieros.

5.2.7 Frecuencia de las revaluaciones

La NIC 38 exige que las revaluaciones se realicen con suficiente regularidad para que, al final del período sobre el que se informa, el importe en libros no

difiera materialmente de su valor razonable. La propia norma reconoce que la frecuencia necesaria dependerá de la volatilidad del activo y que activos con variaciones significativas y volátiles pueden requerir revaluaciones más frecuentes (IFRS Foundation, 2026, NIC 38, párrs. 75 y 79).

Esta disposición posee especial relevancia en el mercado de criptoactivos, caracterizado por movimientos de precio que pueden ser sustanciales en períodos relativamente cortos. La evidencia empírica ha documentado una elevada volatilidad de los precios de las criptomonedas (Garratt & van Oordt, 2023).

En consecuencia, una entidad que aplique válidamente el modelo de revaluación no debería limitarse mecánicamente a actualizar el valor una vez al año si, debido a la volatilidad del activo, ello produce diferencias materiales respecto del valor razonable al cierre.

5.2.8 Vida útil y amortización de criptoactivos clasificados como intangibles

La medición posterior bajo la NIC 38 requiere además determinar si el activo posee una vida útil finita o indefinida. La norma establece que un activo intangible posee vida útil indefinida cuando, considerando todos los factores relevantes, no existe un límite previsible para el período durante el cual se espera que genere entradas netas de efectivo para la entidad (IFRS Foundation, 2026, NIC 38, párr. 88).

Si la vida útil es finita, el activo se amortiza sistemáticamente durante dicha vida útil. Si la vida útil es indefinida, no se amortiza, pero queda sujeto al régimen de deterioro establecido por la NIC 36 (IFRS Foundation, 2026, NIC 38; IFRS Foundation, 2026, NIC 36).

En el caso de las criptomonedas, no debe asumirse automáticamente una vida útil indefinida por el simple hecho de que el protocolo no establezca una fecha formal de vencimiento. La entidad debe considerar las características del activo, restricciones contractuales o legales, cambios tecnológicos, obsolescencia, continuidad de la red, expectativas de utilización y demás factores relevantes.

Asimismo, la determinación de vida útil debe ser revisada periódicamente. En un ecosistema tecnológico altamente cambiante, la desaparición de mercados, abandono de protocolos, pérdida de utilidad económica o cambios regulatorios pueden alterar significativamente las expectativas iniciales.

5.2.9 Deterioro de criptoactivos contabilizados bajo la NIC 38

Los criptoactivos clasificados como activos intangibles quedan sujetos a la NIC 36 Deterioro del Valor de los Activos. El principio central de esta norma consiste en que ningún activo debe presentarse por un importe superior a aquel que pueda recuperarse mediante su utilización o venta. Cuando el importe en libros supera su importe recuperable, existe deterioro y debe reconocerse la pérdida correspondiente (IFRS Foundation, 2026, NIC 36).

El importe recuperable corresponde al mayor entre:

a) El valor razonable menos los costos de disposición; y

b) El valor en uso.

Para los activos intangibles con vida útil indefinida, la NIC 36 exige realizar una prueba de deterioro al menos anualmente, independientemente de que existan indicios específicos de deterioro. Para otros activos, la prueba se efectúa cuando existen indicadores de que el importe en libros podría no ser recuperable (IFRS Foundation, 2026, NIC 36).

En materia de criptoactivos, entre las circunstancias que podrían requerir un análisis especialmente cuidadoso se encuentran reducciones significativas de precios, pérdida sustancial de liquidez, interrupciones de una red, desaparición de mercados relevantes, vulnerabilidades tecnológicas severas o eventos que comprometan la capacidad de realización económica del activo.

Debe enfatizarse, sin embargo, que una disminución temporal de cotización no equivale automáticamente a una pérdida por deterioro. La entidad debe aplicar los requisitos específicos de la NIC 36 y determinar el importe recuperable.

5.2.10 Medición de criptoactivos clasificados como inventarios

Cuando las criptomonedas son mantenidas para su venta en el curso ordinario de las operaciones, el IFRS Interpretations Committee concluyó que corresponde aplicar la NIC 2 (IFRS Interpretations Committee, 2019).

La regla general de la NIC 2 establece que los inventarios se medirán al menor entre el costo y el valor neto realizable (IFRS Foundation, 2026, NIC 2).

Por tanto:

Importe del inventario = min(Costo, Valor neto realizable)

El valor neto realizable corresponde al precio estimado de venta dentro del curso ordinario del negocio menos los costos estimados necesarios para realizar dicha venta (IFRS Foundation, 2026, NIC 2).

Ejemplo práctico

Una empresa dedicada ordinariamente a comercializar determinados criptoactivos mantiene unidades cuyo costo acumulado asciende a US$ 100,000. Al cierre:

Precio estimado de venta: US$ 92,000

Costos necesarios para realizar la venta: US$ 2,000

Valor neto realizable: US$92,000 -US$2,000 = US\ 90,000

Como el valor neto realizable es inferior al costo (Costo: US$ 100,000 vs. VNR: US$ 90,000), el inventario debe ajustarse y la reducción de US$ 10,000 deberá reconocerse conforme a los requerimientos de la NIC 2.

5.2.11 Criptoactivos mantenidos por broker-traders

La NIC 2 contempla un tratamiento especial para los intermediarios que comercian con materias primas (*commodity broker-traders*). El IFRS Interpretations Committee señaló específicamente que una entidad que actúe como *broker-trader* de criptomonedas debe considerar los requisitos del párrafo 3(b) de la NIC 2. Estos inventarios son adquiridos principalmente con la finalidad de venderlos en el futuro próximo y obtener beneficios derivados de las fluctuaciones de precios o del margen del intermediario (IFRS Interpretations Committee, 2019).

Cuando se satisfacen esas condiciones, los inventarios se miden a valor razonable menos los costos de venta, y los cambios en dicha medición se reconocen en los resultados del período correspondiente.

Este tratamiento resulta sustancialmente diferente de:

La regla general del menor entre costo y valor neto realizable de la NIC 2.

El modelo del costo o de revaluación de la NIC 38.

Por esta razón, la calificación de una entidad como *broker-trader* no debe inferirse simplemente del hecho de que realice numerosas compraventas. Deben evaluarse la naturaleza de su actividad, el propósito de las adquisiciones, el modelo de negocio y las condiciones establecidas por la NIC 2.

5.2.12 Determinación del costo de los inventarios de criptoactivos

Cuando corresponda aplicar la NIC 2, el costo comprende los costos de adquisición y otros costos incurridos para llevar los inventarios a su ubicación y condición actuales (IFRS Foundation, 2026, NIC 2).

Otro problema particularmente relevante corresponde a determinar qué costo debe asignarse a las unidades vendidas cuando la entidad ha adquirido un mismo criptoactivo en diferentes fechas y a distintos precios.

La NIC 2 contempla la identificación específica para inventarios que no sean ordinariamente intercambiables y, para los elementos intercambiables, permite fórmulas como FIFO (primeras entradas, primeras salidas) o promedio ponderado (IFRS Foundation, 2026, NIC 2).

La trazabilidad tecnológica de cada movimiento en *blockchain* no modifica por sí sola las reglas contables sobre fórmulas de costo. Por ejemplo, la posibilidad técnica de seguir determinadas unidades o salidas desde una *wallet* no significa necesariamente que pueda seleccionarse arbitrariamente el costo histórico más conveniente para determinar el resultado contable. La entidad debe documentar y aplicar consistentemente la política de costo requerida por la norma.

5.2.13 Valor razonable bajo la NIIF 13

La NIIF 13 Medición del Valor Razonable no determina qué activos deben medirse a valor razonable. Su función consiste en establecer cómo debe determinarse el valor razonable cuando otra NIIF exige o permite utilizarlo (IFRS Foundation, 2026, NIIF 13).

La NIIF 13 define el valor razonable como el precio que se recibiría por vender un activo o que se pagaría por transferir un pasivo en una transacción ordenada entre participantes del mercado en la fecha de medición (IFRS Foundation, 2026, NIIF 13, párr. 24).

De esta definición se desprenden varios elementos esenciales:

Valor razonable= Precio de salida+ Perspectiva de mercado+ Fecha específica de medición+ Transacción ordenada}$$

No representa el precio que la entidad desea obtener, ni necesariamente el importe pagado originalmente, ni un valor calculado exclusivamente desde sus expectativas internas.

5.2.14 Mercado principal y mercado más ventajoso

Una de las mayores dificultades en la valoración de criptoactivos surge porque un mismo activo puede negociarse simultáneamente en diversos *exchanges* con precios, volúmenes y niveles de liquidez diferentes.

La NIIF 13 establece que la medición debe realizarse en el mercado principal del activo o, cuando no exista un mercado principal, en el mercado más ventajoso al cual la entidad tenga acceso. El mercado principal corresponde al mercado con mayor volumen y nivel de actividad para el activo o pasivo (IFRS Foundation, 2026, NIIF 13).

Por tanto, una entidad no debería limitarse a seleccionar, al cierre del ejercicio, el *exchange* que presente el precio más alto con la finalidad de aumentar la valoración de sus activos. Debe identificar previamente el mercado pertinente conforme a la NIIF 13.

Ejemplo analítico de selección de mercado

Supóngase que Bitcoin cotiza de la siguiente manera:

Plataforma	Precio BTC	Volumen y actividad
Exchange A	US$ 70,100	Muy alto
Exchange B	US$ 70,600	Bajo
Exchange C	US$ 69,950	Alto

No sería correcto utilizar automáticamente US$ 70,600 solo por ser la mayor cotización. Primero debe identificarse cuál constituye el mercado principal accesible para la entidad (en este caso, el Exchange A, debido a su mayor volumen y nivel de actividad).

Este requerimiento adquiere especial importancia en el ecosistema de criptoactivos debido a su fragmentación entre plataformas, redes y mecanismos de negociación. El Banco de Pagos Internacionales ha señalado que el ecosistema cripto presenta fragmentación entre plataformas y redes, lo cual incrementa la relevancia de analizar adecuadamente las fuentes de precios utilizadas (Bank for International Settlements [BIS], 2023)s.

5.2.15 Accesibilidad al mercado

No basta con que exista un mercado de gran volumen a nivel mundial. La entidad debe poder acceder a ese mercado en la fecha de medición.

En el ámbito de los criptoactivos, esta condición puede verse afectada por:

- Restricciones territoriales de determinados *exchanges*
- Requisitos de identificación del cliente
- Restricciones regulatorias
- Prohibiciones para determinados tipos de personas jurídicas
- Límites de retiro
- Suspensión temporal de operaciones

- Restricciones sobre determinados tokens
- Diferencias entre mercados institucionales y minoristas

En consecuencia, utilizar el precio de una plataforma a la cual la entidad no posee acceso efectivo puede resultar incompatible con el enfoque establecido por la NIIF 13.

5.2.16 Precio de cierre y mercados que funcionan permanentemente

A diferencia de muchos mercados financieros tradicionales, los mercados de criptoactivos funcionan generalmente de forma continua. No existe necesariamente una única "campana de cierre" universal.

Esta característica genera un problema contable relevante: ¿qué precio debe utilizarse a la fecha de cierre del estado de situación financiera?

La respuesta exige establecer una metodología consistente que determine:

- Fecha exacta de medición
- Zona horaria
- Hora de corte
- Mercado principal
- Par de negociación utilizado
- Fuente de datos

Procedimiento aplicable cuando existen operaciones alrededor del momento de cierre

Por ejemplo, para estados financieros terminados el 31 de diciembre, no debería seleccionarse discrecionalmente entre el precio más alto, el más bajo o el promedio de ese día con la finalidad de producir determinado resultado.

La política contable debe establecer una metodología reproducible y consistente que represente las condiciones de mercado existentes en la fecha de medición.

Desde una perspectiva forense, debe conservarse evidencia del dato utilizado: fuente, fecha, hora, *exchange*, mercado, moneda o activo de cotización y mecanismo utilizado para obtenerlo.

5.2.17 Costos de transacción y valor razonable

La NIIF 13 establece una diferenciación particularmente importante: los costos de transacción no se deducen del precio utilizado para medir el valor razonable, porque no constituyen una característica del activo, sino de la operación

específica mediante la cual se realiza la venta (IFRS Foundation, 2026, NIIF 13, párr. 25).

Por consiguiente:

Valor razonable=Precio de mercado−costos de transacción

(Nota: Los costos de transacción no se deducen para determinar el valor razonable per se, pero aplican en definiciones específicas de valor neto realizable o valor razonable menos costos de venta).

No obstante, cuando otra norma establece expresamente una medición de valor razonable menos costos de venta, como ocurre en determinadas circunstancias de la NIC 2 para *broker-traders*, los costos correspondientes sí deben considerarse para obtener esa medición específica.

Por ello debe evitarse confundir el valor razonable con el valor razonable menos costos de venta.

5.2.18 Jerarquía del valor razonable

La NIIF 13 establece una jerarquía de tres niveles para los datos utilizados en la valoración. La clasificación pretende incrementar la consistencia y comparabilidad de las mediciones, otorgando máxima prioridad a precios cotizados no ajustados en mercados activos para activos idénticos y menor prioridad a datos no observables (IFRS Foundation, 2026, NIIF 13, párrs. 72-90).

Nivel 1

Corresponde a precios cotizados, sin ajustar, en mercados activos para activos o pasivos idénticos a los cuales la entidad puede acceder en la fecha de medición.

Cuando un criptoactivo se negocia en un mercado que satisface estas condiciones, el precio observable puede constituir un dato de Nivel 1. Sin embargo, una cotización de un *exchange* no es automáticamente un dato de Nivel 1. Debe demostrarse que:

- Corresponde al mismo activo
- El mercado está activo
- La entidad puede acceder al mercado
- El precio corresponde a la fecha de medición

Se ha identificado correctamente el mercado principal o más ventajoso, según corresponda

Nivel 2

Incluye datos observables distintos de los precios cotizados de Nivel 1. Puede comprender, dependiendo de las circunstancias, precios de activos similares, precios observables en mercados que no satisfacen los requisitos para calificarse como activos o determinados parámetros observables utilizados en modelos de valoración.

Nivel 3

Comprende datos no observables utilizados cuando existe poca o ninguna actividad de mercado relevante para la medición. En estos casos se incrementa significativamente el nivel de juicio profesional.

Puede resultar particularmente relevante para:

- Tokens con escasa negociación
- Determinados NFT
- Tokens representativos de derechos específicos
- Criptoactivos emitidos recientemente
- Activos tokenizados sin mercado líquido
- Determinados instrumentos DeFi

Una medición de Nivel 3 exige especial atención a las hipótesis utilizadas y a las revelaciones correspondientes.

5.2.19 Técnicas de valoración cuando no existe un precio directamente observable

Cuando no existe un precio observable adecuado, la NIIF 13 permite utilizar técnicas de valoración apropiadas a las circunstancias y para las cuales existan datos suficientes. Entre los enfoques reconocidos se encuentran el enfoque de mercado, el enfoque de ingresos y el enfoque del costo (IFRS Foundation, 2026, NIIF 13).

En materia de criptoactivos, la selección de la metodología deberá guardar relación con la sustancia económica del activo:

- **Enfoque de mercado:** Puede utilizar precios y otra información derivada de operaciones con activos idénticos o comparables. Resulta especialmente pertinente cuando existen transacciones observables suficientes.
- **Enfoque de ingresos:** Convierte importes futuros por ejemplo, flujos de efectivo en un valor presente. Podría resultar relevante para determinados tokens que incorporen derechos económicos sobre flujos futuros, siempre que la naturaleza contractual del instrumento justifique dicha metodología.

- **Enfoque del costo:** Busca reflejar el importe requerido actualmente para sustituir la capacidad de servicio del activo. Su aplicación a determinados criptoactivos puede ser limitada, dado que el costo técnico de crear un token no necesariamente guarda relación con su valor económico.

En consecuencia, no existe un modelo universal de valoración aplicable indistintamente a Bitcoin, *stablecoins*, NFT, *utility tokens*, *security tokens* y activos del mundo real tokenizados.

5.2.20 Valoración de *stablecoins*

La denominación *stablecoin* tampoco permite asumir automáticamente que su valor contable equivale en todo momento a la moneda de referencia.

Aunque determinadas *stablecoins* pretenden mantener una paridad por ejemplo, una unidad por un dólar estadounidense, su medición debe considerar la naturaleza económica y contractual del instrumento. Será necesario analizar:

- Existencia de emisor
- Activos de respaldo
- Derecho jurídico de reembolso
- Condiciones de rescate
- Riesgo de crédito
- Liquidez
- Restricciones al reembolso
- Precio observable en mercados
- Existencia de desviaciones respecto de la paridad
- Norma contable aplicable

El *Financial Stability Board* ha señalado que los acuerdos de *stablecoins* presentan características y riesgos propios que requieren regulación y supervisión específicas, por lo que no resulta adecuado equipararlas automáticamente con efectivo simplemente porque aspiren a mantener un valor estable (Financial Stability Board [FSB], 2023).

Así, una *stablecoin* con derecho contractual exigible frente a un emisor puede conducir a una evaluación contable diferente de una *stablecoin* algorítmica cuya estabilidad dependa de mecanismos de mercado y no de un derecho de reembolso contractual.

5.2.1 Valoración de NFT

Los tokens no fungibles presentan dificultades adicionales debido a que, por definición, su individualización puede reducir considerablemente la disponibilidad de operaciones con activos idénticos.

La última transacción de un NFT no necesariamente representa su valor razonable actual, particularmente cuando:

- La operación ocurrió hace un período significativo
- El mercado perdió liquidez
- Existen pocas transacciones comparables
- Las características del activo son únicas
- La contraparte fue relacionada
- La operación no puede considerarse representativa de una transacción ordenada

Por ello, la determinación del valor razonable de determinados NFT puede requerir técnicas de valoración con un mayor componente de datos no observables y, consecuentemente, situarse en niveles inferiores de la jerarquía del valor razonable.

No resulta técnicamente adecuado extrapolar automáticamente el precio de un NFT a otro simplemente porque ambos pertenezcan a la misma colección.

5.2.2 Valoración de activos del mundo real tokenizados

En los *real-world assets* (RWA), la valoración debe considerar prioritariamente el activo o derecho económico subyacente. Por ejemplo:

- Un token que representa deuda deberá analizarse según las características del instrumento financiero
- Un token representativo de una participación patrimonial requerirá analizar los derechos societarios correspondientes
- Un token respaldado por oro requerirá analizar qué derecho posee realmente el titular sobre el metal
- Un token vinculado a un inmueble exige determinar si representa propiedad, participación, derecho contractual sobre ingresos u otra relación jurídica

En consecuencia, tokenizar un activo no crea necesariamente una nueva base de medición contable. La *blockchain* puede modificar la forma en que el derecho se representa, registra o transfiere, pero la base de valoración conti-

nuará dependiente de la sustancia económica del activo o derecho controlado por la entidad.

5.2.3 Criptoactivos que califican como instrumentos financieros

Cuando un token satisface la definición de activo financiero, su medición deja de estar determinada por la NIC 38 o la NIC 2 y debe evaluarse bajo la normativa aplicable a instrumentos financieros.

La NIIF 9 establece que los activos financieros se clasifican y miden considerando el modelo de negocio mediante el cual son gestionados y las características de sus flujos de efectivo contractuales. Dependiendo de dichas condiciones, pueden medirse al costo amortizado, a valor razonable con cambios en otro resultado integral o a valor razonable con cambios en resultados (IFRS Foundation, 2026, NIIF 9).

Este análisis puede resultar especialmente relevante para determinados:

- Tokens de deuda
- *Security tokens*
- Instrumentos financieros tokenizados
- Derechos contractuales digitalizados
- Determinadas *stablecoins* con derechos contractuales

Debe insistirse nuevamente en que la aplicación de la NIIF 9 depende de los derechos contractuales, y no de que el instrumento utilice *blockchain*.

5.2.4 Diferencias de precios entre *exchanges*

La coexistencia de precios diferentes para el mismo criptoactivo constituye uno de los principales desafíos prácticos de valoración. Las diferencias pueden estar relacionadas, entre otros factores, con:

- Liquidez
- Volumen
- Restricciones de acceso
- Moneda o activo utilizado como par de negociación
- Profundidad del libro de órdenes
- Jurisdicción
- Condiciones operativas del mercado
- Demanda local

Estas circunstancias impiden utilizar indiscriminadamente precios obtenidos de cualquier proveedor de información. Para efectos contables y de auditoría deberá documentarse:

Activo → mercado principal → exchange → par de negociacion → fecha/hora → precio utilizado → fuente de evidencia

Además, la información procedente de agregadores de precios debe evaluarse cuidadosamente. Un precio promedio obtenido de múltiples *exchanges* puede resultar útil como referencia económica, pero no necesariamente representa el precio exigido por la NIIF 13 cuando existe un mercado principal identificable.

5.2.5 Conversión a moneda funcional

La valoración de los criptoactivos debe finalmente expresarse en la moneda funcional de la entidad.

Cuando la cotización utilizada se encuentre expresada en una moneda distinta por ejemplo, BTC/USD y la entidad prepare sus estados financieros en su moneda local, deberá efectuarse la conversión correspondiente aplicando los requisitos de las NIIF sobre moneda extranjera que resulten aplicables.

Desde una perspectiva pericial, deben conservarse separadamente:

- Precio del criptoactivo en la moneda o par de negociación
- Cantidad de unidades
- Importe resultante
- Tipo de cambio utilizado
- Fecha y hora de ambos valores
- Fuente de información

Una práctica deficiente consiste en utilizar simultáneamente cotizaciones correspondientes a diferentes horas o fechas, generando un valor que nunca existió efectivamente en el mercado.

5.2.6 Eventos posteriores y volatilidad de precios

Debido a la volatilidad de los activos virtuales, pueden producirse variaciones sustanciales entre la fecha de cierre y la fecha de autorización de los estados financieros.

El *IFRS Interpretations Committee* recordó expresamente que las entidades que mantienen criptomonedas deben considerar los requerimientos sobre hechos ocurridos después del período sobre el que se informa, incluyendo la ne-

cesidad de revelar cambios significativos de valor posteriores al cierre cuando constituyan hechos no ajustables cuya omisión pudiera influir en las decisiones de los usuarios (IFRS Interpretations Committee, 2019).

Por tanto, el hecho de que el precio de un criptoactivo aumente o disminuya considerablemente después de la fecha de cierre no significa automáticamente que deba modificarse su valor al cierre. Debe diferenciarse entre:

- Condiciones existentes en la fecha de medición
- Acontecimientos surgidos posteriormente

La distinción es fundamental para evitar incorporar información retrospectiva improcedente en la valoración.

5.2.7 Riesgos de manipulación o falta de representatividad del precio

Desde una perspectiva de auditoría forense, la existencia de un precio publicado no elimina la necesidad de evaluar su confiabilidad.

Debe analizarse si la transacción o mercado utilizado representa adecuadamente una transacción ordenada y si la información posee suficiente calidad para sustentar la valoración. La NIIF 13 parte precisamente del supuesto de una transacción ordenada entre participantes del mercado, no de una liquidación forzada o una operación realizada bajo condiciones anómalas (IFRS Foundation, 2026, NIIF 13).

El riesgo aumenta respecto de activos de baja liquidez, plataformas de reducido volumen o mercados en los cuales determinadas operaciones puedan alterar significativamente el precio. En estos casos, el auditor o perito deberá evaluar no solamente qué precio aparece, sino cómo se formó ese precio y si resulta representativo del mercado pertinente.

5.2.8 Procedimientos de auditoría y valoración forense

La valoración de activos virtuales requiere integrar información contable, financiera y tecnológica. Un procedimiento forense suficientemente robusto puede estructurarse en las siguientes etapas:

- **Identificación del activo:** Determinar *blockchain*, contrato inteligente cuando corresponda, símbolo, cantidad y características económicas.
- **Confirmación de existencia:** Verificar las unidades mediante registros *blockchain*, custodios, *exchanges* y demás evidencia disponible.

- **Determinación de control:** Establecer que el activo corresponde efectivamente a la entidad.
- **Clasificación contable:** Determinar la NIIF aplicable antes de proceder a su valoración.
- **Identificación de la base de medición:** Costo, valor neto realizable, valor razonable, valor razonable menos costos de venta u otra base exigida.
- **Determinación del mercado pertinente:** Identificar el mercado principal o más ventajoso, cuando corresponda.
- **Obtención de la cotización:** Conservar evidencia de fuente, fecha, hora y par de negociación.
- **Verificación independiente:** Contrastar, cuando sea necesario, la información con fuentes independientes.
- **Conversión monetaria:** Convertir el importe a la moneda funcional mediante una fuente apropiada.
- **Reconciliación:** Contrastar el valor determinado con libros contables, auxiliares, *wallets* y registros de terceros.

Este procedimiento permite evitar una situación frecuente: tener evidencia suficiente de la existencia del criptoactivo, pero insuficiente respecto de su valoración contable.

5.2.9 Matriz general de medición

La siguiente matriz sintetiza los principales escenarios:

Clasificación	Medición inicial	Medición posterior	Norma principal
Criptomoneda como activo intangible	Costo	Modelo del costo o modelo de revaluación si existe mercado activo	NIC 38
Intangible de vida útil finita	Costo	Costo/revaluado menos amortización y deterioro	NIC 38 y NIC 36
Intangible de vida útil indefinida	Costo	No se amortiza; prueba anual de deterioro, sujeto al modelo elegido	NIC 38 y NIC 36
Criptomoneda como inventario ordinario	Costo	Menor entre costo y valor neto realizable	NIC 2
Criptoactivo de *broker-trader* que cumple las condiciones de NIC 2	Según norma aplicable	Valor razonable menos costos de venta	NIC 2 y NIIF 13
Token que constituye activo financiero	Valor razonable inicial conforme a NIIF 9	Costo amortizado, FVOCI o FVTPL, según clasificación	NIIF 9

Clasificación	Medición inicial	Medición posterior	Norma principal
Token/NFT sin mercado activo	Según norma aplicable	Puede requerir técnicas de valoración y datos no observables cuando se exige valor razonable	NIIF 13
Activo tokenizado	Según naturaleza del derecho subyacente	Según la NIIF correspondiente	Norma del activo/derecho subyacente

5.2.10 Ejemplo integral de medición

Supóngase que una entidad adquiere 2 BTC por US$ 45,000 cada uno, con el propósito de mantenerlos como inversión y que, tras analizar las condiciones del apartado 5.1, determina que corresponde aplicar la NIC 38.

Costo inicial: 2 BTC×US$ 45,000=US$ 90,000 (sin considerar en este ejemplo costos adicionales).

Escenario A: precio al cierre US$ 70,000 por BTC

Valor observable: 2×US$ 70,000=US$ 140,000

Si aplica el modelo del costo, la simple apreciación del mercado no implica reconocer automáticamente la diferencia de US$ 50,000 como ganancia.

Si aplica válidamente el modelo de revaluación y se satisfacen todos los requisitos de la NIC 38, deberá determinarse el valor razonable conforme a la NIIF 13 y contabilizarse la revaluación conforme a los párrafos 85 y siguientes de la NIC 38.

Escenario B: precio posterior de US$ 25,000 por BTC

Valor observable: 2×US$ 25,000=US$ 50,000

Si se utiliza el modelo del costo, deberá analizarse el deterioro conforme a la NIC 36 cuando resulte aplicable.

Este ejemplo demuestra por qué resulta incorrecto registrar automáticamente:

Precio de mercado actual−Precio de compra=Ganancia o pérdida

El tratamiento depende de la clasificación del activo y de la base de medición exigida por las NIIF.

5.2.11 Consideraciones particulares para la auditoría forense

Desde una perspectiva forense, la valoración debe ser reproducible, verificable y trazable. Un tercero técnicamente competente debería poder recons-

truir cómo se llegó al importe informado utilizando la documentación conservada por el perito o auditor.

Para ello, el expediente de valoración debería permitir establecer como mínimo:

Cantidad de unidades × Precio válido a la fecha de medición×Tipo de cambio = Valor determinado

Asimismo, deberá conservarse evidencia de:

- Dirección de la *wallet*
- Identificador del activo
- Red *blockchain*
- Cantidad
- *Exchange* o mercado utilizado
- Fuente de precios
- Fecha y hora
- Zona horaria
- Par de negociación
- Metodología de valoración
- Nivel de jerarquía de valor razonable
- Ajustes efectuados
- Conversión a moneda funcional
- Responsable del procedimiento

En una investigación de fraude o lavado de activos, esta metodología posibilita además reconstruir la evolución patrimonial de activos que pudieron haber sido adquiridos a un precio y transferidos, intercambiados o liquidados posteriormente a valores sustancialmente distintos.

5.2.12 Principio de consistencia y prevención de selección oportunista de precios

Una de las mayores amenazas a la confiabilidad de la información financiera sobre criptoactivos es la posibilidad de seleccionar entre múltiples precios disponibles aquel que produzca el resultado contable más conveniente.

Para reducir este riesgo, la entidad debe definir previamente políticas sobre:

- Fuente de precios
- Mercado principal
- Hora de corte
- Tratamiento de mercados temporalmente inactivos
- Conversión monetaria
- Procedimiento ante diferencias significativas entre plataformas
- Jerarquía de fuentes alternativas

Estas políticas deben aplicarse consistentemente de un período a otro, salvo que exista una justificación válida para modificarlas.

Desde una perspectiva de auditoría forense, los cambios de fuente de valoración inmediatamente antes o después de una fecha de cierre, particularmente cuando producen efectos materiales, deberán ser objeto de un examen especial.

5.2.13 Limitaciones del modelo contable actual

El tratamiento actual bajo NIIF presenta determinadas dificultades cuando se aplica a activos virtuales. Particularmente, una criptomoneda económicamente mantenida como inversión puede estar comprendida dentro de la NIC 38, aunque sus características económicas y su negociación difieran significativamente de activos intangibles tradicionales como patentes, licencias o marcas.

Estas dificultades han contribuido al debate internacional acerca de la capacidad de la normativa tradicional sobre intangibles para representar adecuadamente determinados activos de naturaleza digital. De hecho, el IASB mantiene actualmente un proyecto de revisión integral de la NIC 38 dirigido, entre otros objetivos, a analizar su adecuación respecto de nuevos tipos de intangibles y nuevas formas de utilización. A julio de 2026, dicho proyecto continúa en fase de investigación y no ha sustituido ni modificado aún los requerimientos vigentes aplicables a las tenencias de criptomonedas (IFRS Foundation, 2026).

(Nota experta: En el texto original figuraba el término «Interamericana», el cual constituía un error tipográfico o conceptual al referirse al debate global e internacional del IASB).

Esta precisión resulta importante para el presente manual: las propuestas, investigaciones o discusiones del IASB no deben confundirse con normas ya vigentes.

5.2.14 Criterio integrador de medición y valoración

La medición de los activos virtuales debe efectuarse mediante un proceso secuencial y fundamentado. Primero se determina la naturaleza económica y clasificación contable del recurso; posteriormente se identifica la base de medición exigida por la norma aplicable; finalmente se determina el importe correspondiente utilizando información fiable y verificable.

Este proceso puede sintetizarse de la siguiente manera:

Identificación del activo → clasificación contable → norma aplicable → base de medición → mercado pertinente → fuente de precio → fecha y hora → conversión monetaria → ajustes normativos → registro contable → evidencia de auditoría

En consecuencia, el valor observable de mercado constituye solamente uno de los elementos del análisis. No todo activo virtual debe medirse a valor razonable, ni toda fluctuación de precio debe reconocerse inmediatamente en resultados.

Para las criptomonedas comprendidas dentro de la decisión del IFRS Interpretations Committee, la medición dependerá principalmente de si corresponde aplicar la NIC 38 o la NIC 2. Cuando exista un instrumento financiero, deberá analizarse la NIIF 9; y cuando una norma exija o permita utilizar el valor razonable, su determinación deberá sujetarse a la NIIF 13 (IFRS Interpretations Committee, 2019; IFRS Foundation, 2026).

Desde la perspectiva de la auditoría forense, la valoración debe incorporar además criterios de integridad, trazabilidad, reproducibilidad y suficiencia probatoria, debido a que una cifra contablemente correcta pero sustentada en una fuente de precios no verificable, un mercado inadecuado o una fecha incorrecta puede comprometer la fiabilidad de los estados financieros y de cualquier conclusión pericial derivada de ellos.

Finalmente, la especial volatilidad y fragmentación de los mercados de criptoactivos exige un nivel elevado de juicio profesional. La metodología adoptada deberá encontrarse suficientemente documentada para demostrar no solamente cuánto vale el activo, sino también por qué ese valor constituye la medición contablemente apropiada en una fecha determinada.

5.3 Registro de operaciones con criptomonedas

El registro contable de las operaciones con criptomonedas constituye uno de los aspectos de mayor complejidad dentro de la información financiera relacionada con activos virtuales. Esta dificultad no deriva únicamente de la volatilidad de sus precios, sino también de las múltiples formas en que pueden ser adquiridas, transferidas, intercambiadas, utilizadas como medio de pago, recibidas como contraprestación, depositadas en plataformas de custodia o empleadas dentro de protocolos descentralizados.

Desde la perspectiva de las Normas Internacionales de Información Financiera (NIIF), no existe un sistema autónomo de contabilización aplicable a todas las operaciones realizadas mediante *blockchain*. El tratamiento depende de la naturaleza económica de la transacción y de la clasificación del activo

involucrado. Para las criptomonedas comprendidas en la decisión del IFRS Interpretations Committee de junio de 2019, la NIC 2 resulta aplicable cuando son mantenidas para la venta en el curso ordinario del negocio y, cuando esa norma no resulta aplicable, corresponde utilizar la NIC 38 (IFRS Interpretations Committee, 2019).

(Nota experta: Se corrige «Normas Interamericanaes» por el término correcto «Normas Internacionales»).

Por consiguiente, una misma transferencia registrada técnicamente en una *blockchain* puede representar fenómenos contables completamente diferentes: adquisición de un activo, venta, intercambio de activos no monetarios, pago de una obligación, transferencia entre *wallets* propias, comisión por transacción, distribución gratuita, recompensa de un protocolo o simplemente un movimiento de custodia que no produce modificación patrimonial.

La contabilización debe partir, por ello, de un principio fundamental: **una transacción *blockchain* no equivale necesariamente a una transacción contable.**

Del mismo modo, una operación económicamente relevante puede encontrarse constituida por varias transacciones *blockchain* o, incluso, ejecutarse íntegramente dentro de los registros internos de un *exchange* sin generar inmediatamente una operación *on-chain*.

5.3.1 Principios para el registro contable de operaciones con criptomonedas

Antes de efectuar un asiento contable relacionado con criptoactivos, la entidad debe determinar la sustancia económica del hecho y establecer, como mínimo, cinco elementos: el activo o derecho involucrado, la entidad que lo controla, la norma contable aplicable, la base de medición y el momento en que se produce el reconocimiento o baja.

Cuando ninguna NIIF regule específicamente una determinada operación, la NIC 8 requiere que la gerencia ejerza juicio profesional para desarrollar una política contable que proporcione información relevante y fiable. Para ello debe considerar, en orden jerárquico, los requerimientos de las NIIF relativos a cuestiones similares y relacionadas y los criterios contenidos en el Marco Conceptual (IFRS Foundation, s. f.).

Esta disposición adquiere particular importancia respecto de operaciones como minería, *staking*, *airdrops*, *hard forks*, protocolos de finanzas descentralizadas (DeFi), provisión de liquidez o determinadas estructuras de tokenización,

para las cuales no existe actualmente una norma NIIF integral que establezca un único tratamiento contable.

En consecuencia, el proceso lógico de registro puede expresarse como:

Hecho económico → identificación de derechos y obligaciones → reconocimiento → clasificación → medición → registro contable → documentación → conciliación → revelación

5.3.2 Importancia del registro auxiliar de criptoactivos

La contabilidad general debería complementarse con un registro auxiliar o *subledger* de activos virtuales que permita conciliar permanentemente la información financiera con las *wallets*, *exchanges*, custodios y registros *blockchain*.

Este registro auxiliar debería contener, como mínimo, los siguientes campos:

Información	Finalidad
Tipo de criptoactivo	Identificación económica
Símbolo	BTC, ETH, USDC, etc.
Blockchain o red	Bitcoin, Ethereum u otra
Dirección de *wallet*	Identificación del origen o destino
Exchange/custodio	Determinación de la ubicación o custodia
Fecha y hora	Determinación del período contable
Zona horaria	Evitar errores de corte
Transaction hash (TxID)	Trazabilidad *blockchain*
Tipo de operación	Compra, venta, intercambio, transferencia, recompensa, etc.
Unidades ingresadas	Control cuantitativo
Unidades retiradas	Control cuantitativo
Comisión	Determinación del costo
Costo histórico	Seguimiento contable
Valor razonable (cuando proceda)	Medición
Contraparte identificada	Trazabilidad económica
Documento de soporte	Evidencia
Asiento contable relacionado	Conciliación con libro mayor

Este auxiliar es especialmente importante porque el saldo visible en una *blockchain* expresa fundamentalmente unidades de activos, mientras que la contabilidad necesita además expresar dichas unidades en la moneda funcional de la entidad.

Por ello debe cumplirse permanentemente la igualdad:

- Cantidad de criptoactivos acreditada documentalmente=Cantidad registrada en auxiliares=Cantidad incorporada al saldo contable
- *(después de considerar las operaciones pendientes de liquidación o conciliación).*

5.3.3 Compra de criptomonedas mediante moneda fiduciaria

Cuando una entidad adquiere criptomonedas mediante dinero y, de acuerdo con el análisis efectuado en los apartados anteriores, dichas criptomonedas se contabilizan como activos intangibles conforme a la NIC 38, su reconocimiento inicial se efectúa al costo. La NIC 38 establece que un activo intangible se mide inicialmente al costo y contempla dentro de este los desembolsos directamente atribuibles que correspondan conforme a sus requerimientos (IFRS Foundation, 2021).

Supóngase que una empresa adquiere 1 BTC por 50,000 unidades monetarias (u.m.), pagando además una comisión directamente atribuible de 500 u.m., respecto de la cual se concluye que forma parte del costo.

El registro ilustrativo sería:

Cuenta	Debe	Haber
Criptoactivos – activo intangible	50,500	—
Efectivo/Bancos	—	50,500

El saldo inicial del criptoactivo será, en este supuesto, 50,500 u.m.

El asiento constituye solamente una representación genérica. La denominación y codificación de las cuentas debe adecuarse al plan de cuentas y legislación contable de cada jurisdicción.

La evidencia de esta adquisición debería permitir vincular el desembolso bancario con la orden ejecutada en el *exchange* y, posteriormente, con la tenencia acreditada en la cuenta del *exchange* o en la *wallet* correspondiente.

5.3.1 Compra de criptomonedas clasificadas como inventarios

Cuando la entidad mantiene criptomonedas para la venta dentro del curso ordinario de sus operaciones, el IFRS Interpretations Committee determinó que corresponde aplicar la NIC 2 (IFRS Interpretations Committee, 2019).

La NIC 2 establece que el costo de los inventarios comprende los costos de adquisición y demás costos incurridos para llevarlos a su ubicación y condición actuales. Asimismo, establece como regla general la medición posterior al menor entre costo y valor neto realizable (IFRS Foundation, s. f.).

Supóngase la compra de activos virtuales destinados a comercialización ordinaria por 80,000 u.m., incluidos los costos que satisfacen los requisitos para formar parte de su costo:

Cuenta	Debe	Haber
Inventarios – criptoactivos	80,000	—
Efectivo/Bancos	—	80,000

En este escenario, el criptoactivo no debería contabilizarse simultáneamente como activo intangible e inventario. La clasificación efectuada al momento de determinar la política contable condiciona los registros posteriores.

5.3.2 Registro de la venta de criptomonedas contabilizadas bajo la NIC 38

Cuando una criptomoneda reconocida como activo intangible es vendida, la NIC 38 exige darla de baja. La ganancia o pérdida se determina mediante la diferencia entre el importe neto obtenido por su disposición y el importe en libros del activo, reconociéndose dicha diferencia en resultados. La norma establece, además, que la ganancia derivada de la baja no debe presentarse como ingreso ordinario (IFRS Foundation, 2021, NIC 38, párrs. 112-113).

Supóngase que una entidad posee un criptoactivo cuyo importe en libros asciende a 35,000 u.m. y lo vende por 50,000 u.m.

La diferencia es:

US$ 50,000−US$ 35,000=US$ 15,000 u.m. de ganancia

Registro ilustrativo:

Cuenta	Debe	Haber
Efectivo/Bancos	50,000	—

Cuenta	Debe	Haber
Criptoactivos – activo intangible	—	35,000
Ganancia por disposición de criptoactivos	—	15,000

Esta distinción es importante: las 15,000 u.m. no constituyen ventas o ingresos ordinarios simplemente porque exista una utilidad económica en la operación. Bajo el supuesto planteado, representan una ganancia derivada de la baja de un activo intangible conforme a la NIC 38.

Si el importe recibido fuera inferior al importe en libros, la diferencia se reconocería como pérdida.

5.3.3 Registro de la venta de criptomonedas consideradas inventarios

El tratamiento cambia sustancialmente cuando los criptoactivos constituyen inventarios mantenidos para la venta en el curso ordinario del negocio.

La NIC 2 establece que, cuando los inventarios son vendidos, su importe en libros debe reconocerse como gasto durante el mismo período en que se reconoce el ingreso relacionado (IFRS Foundation, s. f.).

Supóngase que un comerciante de criptoactivos vende por 50,000 u.m. criptomonedas cuyo costo asciende a 35,000 u.m.

El registro puede representarse mediante dos efectos:

1. Reconocimiento de la venta

Cuenta	Debe	Haber
Efectivo/Cuentas por cobrar	50,000	—
Ingresos por venta de criptoactivos	—	50,000

2. Reconocimiento del costo

Cuenta	Debe	Haber
Costo de venta de criptoactivos	35,000	—
Inventarios – criptoactivos	—	35,000

Resultado bruto:

50,000−35,000=15,000 u.m.

La diferencia con el supuesto anterior es relevante. Cuando el activo se encontraba contabilizado bajo la NIC 38, se reconoció una ganancia por disposición; cuando constituye inventario vendido dentro de la actividad ordinaria, se

reconoce el ingreso correspondiente y separadamente el costo del inventario vendido.

5.3.4 Entidades que actúan como *broker-traders*

El IFRS Interpretations Committee también reconoció que determinadas entidades pueden actuar como *broker-traders* de criptomonedas. En estas circunstancias debe evaluarse el párrafo 3(b) de la NIC 2, aplicable a intermediarios que adquieren inventarios principalmente para venderlos en un futuro próximo y obtener beneficios procedentes de las fluctuaciones de precios o del margen de intermediación (IFRS Interpretations Committee, 2019).

Cuando se cumplen los requisitos correspondientes, dichos inventarios se miden a valor razonable menos costos de venta, reconociéndose las variaciones en resultados.

Por ejemplo, si el valor en libros de los criptoactivos de un *broker-trader* es de 100,000 u.m. y al cierre el valor razonable menos costos de venta asciende a 115,000 u.m., la variación sería:

Cuenta	Debe	Haber
Inventarios – criptoactivos	15,000	—
Ganancia por medición a valor razonable	—	15,000

Si la medición disminuyera, el registro se produciría en sentido contrario.

No debe utilizarse este tratamiento únicamente porque una empresa efectúe operaciones frecuentes con criptomonedas; deben satisfacerse las condiciones previstas por la NIC 2 para este tipo de intermediarios.

5.3.5 Recepción de criptomonedas como pago por bienes o servicios

Las criptomonedas también pueden constituir la contraprestación recibida por una entidad a cambio de bienes o servicios.

La NIIF 15 establece que una entidad reconoce ingresos de manera que represente la transferencia de los bienes o servicios comprometidos al cliente por un importe que refleje la contraprestación a la que espera tener derecho. Cuando la contraprestación es no monetaria, la NIIF 15 establece su medición a valor razonable, sujeto a los requerimientos específicos de la norma (IFRS Foundation, 2022; IFRS Foundation, 2024).

Supóngase que una empresa presta un servicio y recibe 0.20 BTC, cuyo valor razonable determinado conforme a la política aplicable asciende a 12,000 u.m.

Registro ilustrativo:

Cuenta	Debe	Haber
Criptoactivos	12,000	—
Ingresos por servicios	—	12,000

A partir de ese momento existen dos fenómenos contables distintos:

El ingreso, determinado por la transacción con el cliente.

El criptoactivo recibido, cuyo tratamiento posterior dependerá de su clasificación bajo la norma correspondiente.

Si posteriormente el criptoactivo aumenta a 15,000 u.m., las 3,000 u.m. de diferencia no constituyen ingresos adicionales por el servicio originalmente prestado. Constituyen una variación posterior del activo y deberán tratarse conforme a la NIC 38, NIC 2, NIIF 9 u otra norma que resulte aplicable.

5.3.6 Pago de obligaciones mediante criptomonedas

El pago de una deuda mediante criptomonedas implica analizar simultáneamente la extinción de la obligación y la disposición del activo utilizado para pagarla.

Supóngase que una entidad mantiene una cuenta por pagar de 40,000 u.m. y entrega para cancelarla una cantidad de criptomonedas cuyo importe en libros es 30,000 u.m., siendo aceptada por el acreedor como cancelación total de la deuda.

De manera simplificada:

Cuenta	Debe	Haber
Cuentas por pagar	40,000	—
Criptoactivos	—	30,000
Ganancia por disposición del criptoactivo	—	10,000

El pago no debe registrarse simplemente como si se hubieran entregado 40,000 u.m. de efectivo. La entidad está disponiendo de un activo no monetario cuyo importe en libros puede diferir del valor atribuido en la transacción.

En consecuencia, utilizar criptomonedas para adquirir un bien, pagar un servicio o cancelar una obligación puede producir un resultado por disposición del criptoactivo, además del reconocimiento del bien, gasto o pasivo correspondiente.

5.3.7 Intercambio de una criptomoneda por otra

Una de las operaciones más frecuentes consiste en intercambiar directamente un criptoactivo por otro (por ejemplo, BTC → ETH o ETH → USDC).

La inexistencia de una conversión intermedia a moneda fiduciaria no elimina el hecho económico ni permite omitirlo de la contabilidad.

Respecto de activos comprendidos en la NIC 38, la norma establece que un intangible adquirido mediante intercambio de activos no monetarios se mide generalmente por su valor razonable, salvo que la operación carezca de sustancia comercial o que el valor razonable de ninguno dos activos pueda medirse de manera fiable. Cuando no procede la medición a valor razonable, el costo del activo recibido se determina a partir del importe en libros del activo entregado (IFRS Foundation, 2021, NIC 38, párrs. 45-47).

Supóngase que una entidad intercambia BTC (importe en libros: 20,000 u.m.; valor razonable: 30,000 u.m.) por ETH cuyo valor razonable asciende también a 30,000 u.m., suponiendo que la operación posee sustancia comercial y se satisfacen los demás requisitos.

Registro ilustrativo:

Cuenta	Debe	Haber
Criptoactivo recibido – ETH	30,000	—
Criptoactivo entregado – BTC	—	20,000
Ganancia por disposición	—	10,000

Este ejemplo demuestra uno de los errores más importantes que puede encontrarse en una investigación contable: considerar que una operación cripto-a-cripto no genera consecuencias contables porque no existió ingreso o salida de dinero bancario.

5.3.8 Transferencias entre *wallets* pertenecientes al mismo titular

Debe diferenciarse claramente un intercambio de una transferencia.

Cuando una entidad traslada Bitcoin desde una *wallet* propia hacia otra *wallet* que también controla y continúa manteniendo el mismo activo y los mismos derechos económicos, no existe, por ese solo hecho, una venta o disposición del activo (ej. de *Wallet corporativa A* a *Wallet corporativa B*).

Por consiguiente, no debería reconocerse una ganancia o pérdida por la variación del precio simplemente como consecuencia de la transferencia.

El registro auxiliar sí deberá actualizarse para identificar la nueva ubicación del activo:

Movimiento auxiliar	BTC
Salida *wallet* A	(1.00)
Entrada *wallet* B	1.00
Variación neta de unidades	**0.00**

Este principio resulta particularmente importante para la auditoría forense. Si las transferencias entre *wallets* propias son contabilizadas erróneamente como ventas y compras, pueden producirse ingresos, costos y resultados ficticios.

5.3.9 Comisiones de red y *gas fees*

Las operaciones *blockchain* pueden generar comisiones pagadas a mineros, validadores o protocolos, conocidas comúnmente como *network fees* o, en determinadas redes, *gas fees*.

Su tratamiento debe determinarse de acuerdo con la naturaleza de la operación a la cual se encuentran vinculadas.

Una comisión directamente atribuible a la adquisición de un activo puede requerir un tratamiento diferente de una comisión originada por una simple transferencia administrativa entre *wallets*. Del mismo modo, los costos relacionados con una venta deben distinguirse de los costos incurridos para adquirir el activo.

Cuando la comisión se paga utilizando otra criptomoneda, existe además una segunda dimensión contable: la entidad está entregando determinadas unidades de un activo virtual. Por tanto, debe eliminar de sus registros las unidades utilizadas para pagar la comisión y determinar el efecto que corresponda según la clasificación y el importe en libros del activo entregado.

Esto puede generar registros más complejos que los producidos por una comisión pagada directamente mediante moneda fiduciaria.

5.3.1 Depósitos y retiros desde *exchanges*

El traslado de criptomonedas desde una *wallet* de autocustodia hacia un *exchange* no debe calificarse automáticamente como venta. Por ejemplo, pasar de una *wallet* propia a una cuenta propia en un *exchange* puede representar simplemente un cambio en la modalidad de custodia si la entidad continúa controlando económicamente el activo.

En sentido contrario, mover fondos de un *exchange* a una *wallet* propia no representa necesariamente una compra; puede constituir únicamente el retiro de un activo previamente adquirido y registrado.

En estos supuestos debe analizarse la relación contractual con la plataforma, porque la naturaleza jurídica y económica del derecho mantenido dentro de un *exchange* puede variar según las condiciones de custodia. Este análisis deberá efectuarse aplicando las NIIF correspondientes y, cuando no exista una norma específicamente aplicable al hecho concreto, los criterios de juicio establecidos por la NIC 8 (IFRS Foundation, s. f.).

Desde la perspectiva forense, este punto resulta crítico porque los sistemas automáticos pueden registrar erróneamente un depósito como venta, o un retiro como compra, cuando económicamente no existe ninguna de esas operaciones.

5.3.2 Operaciones ejecutadas dentro de *exchanges* centralizados

No todas las operaciones realizadas mediante un *exchange* generan inmediatamente una transacción observable en una *blockchain* pública.

Una plataforma centralizada puede registrar internamente compras, ventas e intercambios entre usuarios mediante su propio sistema contable o base de datos. En consecuencia, el análisis exclusivo de la *blockchain* puede no revelar la totalidad de las operaciones efectuadas por una entidad.

Por ello, deben conciliarse conjuntamente:

Registros contables+extractos del exchange+historial de operaciones+depósitos y retiros+movimientos blockchain+saldos finales

La confiabilidad de la evidencia debe evaluarse atendiendo a su fuente, naturaleza y a las circunstancias de su obtención. La NIA 500 exige que el auditor diseñe y ejecute procedimientos para obtener evidencia de auditoría suficiente y adecuada, y reconoce que la fiabilidad de la información utilizada como evidencia depende, entre otros factores, de su procedencia y naturaleza (International Auditing and Assurance Standards Board [IAASB], vigente)s.

5.3.3 Operaciones P2P

Las transacciones *peer-to-peer* (P2P) merecen especial atención porque pueden producirse directamente entre particulares, utilizando simultáneamente transferencias bancarias, billeteras digitales y transferencias *blockchain*.

Por ejemplo, una operación puede estructurarse de la siguiente forma:

transferencia bancaria al vendedor → transferencia de criptoactivo a wallet del comprador

El registro contable debe correlacionar ambos componentes como partes de una misma operación económica.

Desde la perspectiva de prevención del lavado de activos, el GAFI ha destacado específicamente los riesgos relacionados con las operaciones P2P y ha incorporado orientaciones adicionales para su evaluación dentro del ecosistema de activos virtuales (GAFI, 2021).

Para efectos contables y forenses, la inexistencia de un *exchange* intermediario incrementa la importancia de identificar adecuadamente a la contraparte, vincular el pago fiduciario con la transferencia *blockchain* y demostrar el origen y destino económico de los fondos.

5.3.4 Registro de operaciones de minería

La minería introduce un problema diferente porque las criptomonedas pueden ser obtenidas como consecuencia de actividades realizadas dentro de una red y no mediante una compra.

Actualmente, las NIIF no contienen una norma integral específicamente destinada a establecer un tratamiento uniforme para todas las recompensas de minería. En consecuencia, la entidad deberá analizar la sustancia de la actividad y desarrollar una política contable conforme a la jerarquía establecida por la NIC 8 cuando ninguna norma resulte específicamente aplicable (IFRS Foundation, s. f.).

Deberá distinguirse entre los diferentes componentes económicos de la actividad:

- Equipos utilizados en la minería
- Electricidad
- Servicios tecnológicos
- Costos de operación
- Los criptoactivos obtenidos como recompensa

Los equipos informáticos no se convierten en criptoactivos por utilizarse en actividades de minería; su contabilización deberá evaluarse separadamente

conforme a la norma aplicable a dichos activos. De igual forma, los desembolsos operativos no deberían incorporarse automáticamente al costo de las criptomonedas sin verificar previamente si satisfacen los criterios de capitalización correspondientes.

Por ello, la política deberá documentar, como mínimo, cuándo se considera obtenido el control de la recompensa, qué activo se reconoce, cómo se determina su medición inicial y cuál es la naturaleza contable de la contrapartida.

5.3.5 Recompensas por *staking*

Una problemática similar se presenta con el *staking*, mediante el cual determinados titulares bloquean, delegan o comprometen criptoactivos dentro de redes basadas en mecanismos de consenso como *proof of stake*, pudiendo recibir recompensas.

Debe diferenciarse entre, por lo menos, dos situaciones económicamente distintas:

Staking realizado con activos propios directamente frente al protocolo.

Prestación de servicios de *staking* a terceros.

En el segundo supuesto podría existir una relación contractual con un cliente que requiera analizar la NIIF 15. En el primero, la existencia de un "cliente" en los términos de esa norma no debe presumirse automáticamente.

Ante la ausencia de una NIIF específica para todas estas modalidades, el tratamiento deberá desarrollarse conforme a la NIC 8, considerando la naturaleza de la recompensa, el momento de obtención del control, su medición y la clasificación posterior del criptoactivo recibido (IFRS Foundation, s. f.; IFRS Foundation, 2022).

Esta diferenciación evita registrar automáticamente cualquier recompensa de *staking* como "ingreso por ventas", aun cuando la entidad no haya celebrado una operación de venta con un cliente.

5.3.6 *Airdrops* y *hard forks*

Los *airdrops* y *hard forks* representan otra área en la cual no resulta apropiado aplicar un registro automático.

Un *airdrop* puede implicar la recepción de *tokens* sin una contraprestación monetaria directa.

Un *hard fork* puede originar unidades asociadas a una nueva red o protocolo.

La mera aparición técnica de *tokens* en una dirección *blockchain* no demuestra necesariamente que exista un activo que deba reconocerse inmediatamente. La entidad deberá determinar si controla un recurso económico, si dicho recurso reúne las condiciones de reconocimiento y cuál es la política de medición adecuada.

Cuando ninguna NIIF resuelva específicamente la operación, nuevamente resulta aplicable la jerarquía de la NIC 8 (IFRS Foundation, s. f.). Por ello deben evitarse dos extremos:

- Reconocer automáticamente como ingreso todo *token* recibido gratuitamente.
- Ignorar automáticamente dichos *tokens* porque la entidad no pagó por ellos.

La conclusión dependerá de las circunstancias económicas y de la política contable desarrollada sobre bases técnicamente fundamentadas.

5.3.7 Operaciones mediante protocolos DeFi

Las finanzas descentralizadas (DeFi) presentan operaciones que no siempre pueden asimilarse a una simple compra o venta. Entre ellas pueden encontrarse intercambios en *decentralized exchanges* (DEX), provisión de liquidez, préstamos descentralizados, obtención de *tokens* representativos de posiciones económicas, operaciones mediante *smart contracts* y utilización de activos envueltos (*wrapped tokens*).

Cuando una entidad deposita, por ejemplo, ETH en un protocolo y recibe a cambio un *token* que representa su posición, no debería registrarse automáticamente la operación como una mera transferencia de ETH entre dos direcciones. Debe analizarse si:

La entidad continúa controlando esencialmente el mismo recurso, o si, por el contrario,

Ha entregado un activo y obtenido un derecho económicamente diferente.

Esta determinación puede afectar la baja del activo original, el reconocimiento del nuevo activo, su medición y el resultado de la operación.

Debido a que las NIIF no contienen actualmente una norma específica que resuelva universalmente todas las estructuras DeFi, estas operaciones requieren un análisis individual de su sustancia contractual y económica mediante los principios de la NIC 8 y del Marco Conceptual (IFRS Foundation, s. f.).

5.3.1 Pérdida de claves privadas, fraude y sustracción de criptoactivos

La pérdida de una clave privada o *seed phrase* puede tener consecuencias económicas sustanciales porque puede impedir permanentemente que la entidad disponga de los activos asociados. Sin embargo, debe distinguirse entre:

- Pérdida temporal de acceso
- Pérdida irreversible del control
- Robo de credenciales
- Transferencia no autorizada
- Fraude cometido por terceros
- Insolvencia de un custodio

Para activos intangibles, la NIC 38 establece que el activo se dará de baja cuando sea dispuesto o cuando ya no se esperen beneficios económicos futuros de su utilización o disposición (IFRS Foundation, 2021, NIC 38, párr. 112). En el caso de inventarios, la NIC 2 dispone que las pérdidas de inventarios se reconocen como gasto en el período en que ocurren (IFRS Foundation, s. f.).

No obstante, la existencia de una posible reclamación contra un *exchange*, custodio, asegurador u otra parte deberá analizarse separadamente. La baja del criptoactivo y el eventual reconocimiento de un derecho frente a un tercero constituyen fenómenos contables distintos.

Desde una perspectiva forense, resulta indispensable conservar evidencia sobre la última transacción autorizada, direcciones de origen y destino, TxID, mecanismos de acceso, registros de autenticación, documentación del custodio y cronología completa del incidente.

5.3.2 Deterioro de criptoactivos contabilizados como intangibles

Cuando corresponde aplicar la NIC 36, una pérdida por deterioro debe reconocerse cuando el importe en libros supera el importe recuperable del activo. La norma establece que el importe recuperable corresponde al mayor entre el valor razonable menos costos de disposición y el valor en uso (IFRS Foundation, s. f.).

De manera ilustrativa, si un criptoactivo presenta:

Importe en libros: 50,000 u.m.

Importe recuperable determinado conforme a la NIC 36: 32,000 u.m.

La pérdida asciende a:

50,000−32,000=18,000 u.m.

Registro contable del deterioro:

Cuenta	Debe	Haber
Pérdida por deterioro	18,000	—
Deterioro acumulado / Criptoactivo	—	18,000

No debe confundirse este procedimiento con registrar diariamente todas las fluctuaciones negativas del precio como pérdidas por deterioro. Deben satisfacerse rigurosamente los requisitos de la NIC 36.

5.3.3 Registro de la revaluación

Cuando una entidad aplica válidamente el modelo de revaluación previsto por la NIC 38 y existe el mercado activo requerido por esa norma, el incremento del importe en libros se reconoce normalmente en otro resultado integral (ORI) y se acumula en el patrimonio como superávit de revaluación, salvo en la medida en que revierta una disminución anterior reconocida en resultados (IFRS Foundation, 2021, NIC 38).

Por ejemplo, suponiendo que el importe en libros ascienda a 100,000 u.m. y una revaluación válida eleve el importe a 130,000 u.m., sin disminuciones previas reconocidas en resultados:

Cuenta	Debe	Haber
Criptoactivos – activo intangible	30,000	—
Superávit de revaluación – ORI	—	30,000

Este asiento no debe confundirse con la medición de un *broker-trader* bajo la NIC 2, cuyos cambios de valor razonable menos costos de venta se reconocen directamente en resultados.

5.3.4 Transacciones denominadas en criptomonedas y moneda extranjera

También debe diferenciarse una transacción denominada en moneda extranjera de otra cuya contraprestación consiste en criptomonedas.

La NIC 21 define la moneda funcional como la moneda del entorno económico principal en el que opera la entidad y regula la contabilización de las transacciones efectuadas en monedas extranjeras (IFRS Foundation, s. f.). Sin

embargo, las criptomonedas comprendidas en la decisión del IFRS Interpretations Committee de 2019 no fueron consideradas efectivo porque no poseían las características requeridas para ello, ni tampoco fueron calificadas como activos financieros en los supuestos analizados (IFRS Interpretations Committee, 2019).

Por consiguiente, una variación en el precio de Bitcoin no debería contabilizarse automáticamente como diferencia de cambio bajo la NIC 21 simplemente porque su precio se exprese en dólares estadounidenses. Debe distinguirse con claridad:

Variación del valor del criptoactivo=Variación del tipo de cambio de una moneda extranjera

Esta distinción tiene especial relevancia en entidades cuya moneda funcional sea diferente de la moneda utilizada en los mercados para cotizar los criptoactivos.

5.3.5 Operaciones con *tokens* que califican como activos financieros

No todos los activos registrados mediante *blockchain* quedan comprendidos en la decisión del IFRS Interpretations Committee sobre criptomonedas.

Cuando un *token* genera un derecho contractual a recibir efectivo u otro activo financiero, puede corresponder analizar la NIC 32 y la NIIF 9. Esta última exige reconocer un activo financiero cuando la entidad se convierte en parte de las disposiciones contractuales del instrumento y establece su medición inicial y posterior conforme a sus características contractuales y al modelo de negocio de la entidad (IFRS Foundation, s. f.).

En estos casos, el registro de las variaciones posteriores puede producirse al:

- Costo amortizado
- Valor razonable con cambios en otro resultado integral (ORI)
- Valor razonable con cambios en resultados

La consecuencia práctica es significativa: dos *tokens* registrados en una misma *blockchain* pueden generar asientos completamente diferentes porque jurídicamente representan derechos distintos.

5.3.1 Derivados sobre criptomonedas

Las entidades también pueden participar en futuros, opciones, *forwards*, contratos por diferencia u otros derivados cuyo subyacente sea una criptomoneda. En estos casos debe distinguirse claramente:

Tenencia directa del criptoactivoTenencia de un instrumento derivado cuyo valor depende del criptoactivo

La NIIF 9 regula la clasificación y medición de instrumentos financieros y determinados derivados, los cuales generalmente se miden a valor razonable conforme a los requerimientos correspondientes (IFRS Foundation, s. f.). Por ello, no resulta apropiado contabilizar un futuro sobre Bitcoin dentro de la misma cuenta utilizada para Bitcoin mantenido directamente en una *wallet*. La naturaleza económica y contractual de ambos activos es diferente.

5.3.2 Operaciones que no generan flujo de efectivo

Una transacción cripto-a-cripto puede generar efectos económicos y resultados contables sin producir ningún ingreso o salida de efectivo.

La NIC 7 establece que las transacciones de inversión y financiación que no requieren el uso de efectivo o equivalentes de efectivo se excluyen del estado de flujos de efectivo y, cuando corresponda, deben revelarse en otro lugar de los estados financieros de manera que se proporcione información relevante (IFRS Foundation, 2022, NIC 7, párrs. 43-44). Por tanto:

No aparecer en el estado de flujos de efectivoNo existir contablemente

Esto es especialmente importante en los criptoactivos porque una entidad puede realizar numerosas operaciones económicamente significativas sin utilizar cuentas bancarias. Respecto de criptomonedas contabilizadas como activos intangibles, los flujos de efectivo derivados de su adquisición y disposición deberán analizarse considerando la clasificación de actividades de inversión establecida por la NIC 7. Cuando se trate de inventarios adquiridos y vendidos como parte de la actividad ordinaria, la naturaleza del flujo será diferente (IFRS Foundation, s. f.).

5.3.3 Determinación de la fecha y hora del registro

La fecha del registro contable puede presentar dificultades debido a que diferentes eventos tecnológicos pueden ocurrir en momentos distintos:

orden emitida → orden ejecutada → registro interno del exchange → transmisión blockchain → inclusión en bloque → confirmaciones posteriores → disponibilidad efectiva

La entidad debe identificar el momento en que se cumplen los criterios de reconocimiento, transferencia o baja establecidos por la norma correspondiente. La existencia de un *timestamp blockchain* constituye una evidencia importante, pero no siempre es suficiente por sí misma para determinar la fecha del hecho contable.

En operaciones con *exchanges* deben compararse, cuando resulten pertinentes, los siguientes elementos temporales:

Elemento temporal	Utilidad
Fecha y hora de la orden	Inicio de la instrucción
Fecha y hora de ejecución	Formación de la operación
Fecha de liquidación	Cumplimiento contractual
Fecha del movimiento blockchain	Evidencia *on-chain*
Fecha de obtención o pérdida del control	Determinación contable
Zona horaria	Asignación al período correcto

Los errores relacionados con UTC, horario local y fecha de cierre pueden provocar que una misma operación quede registrada en períodos contables diferentes.

5.3.4 Conciliación entre *blockchain* y contabilidad

Una metodología adecuada debería permitir efectuar periódicamente una conciliación entre la cantidad contable y la cantidad tecnológicamente verificable. La ecuación básica puede representarse así:

Saldo inicial de unidades+adquisiciones+recompensas reconocidas+otras entradas−ventas−pagos−comisiones pagadas en cripto−otras salidas=Saldo final teórico

El saldo final teórico debe confrontarse con:

Wallets propias+saldos en exchanges+saldos en custodios+activos comprometidos en protocolos

Las diferencias deben investigarse y no compensarse automáticamente. Una diferencia puede revelar operaciones omitidas, doble contabilización, comisiones no registradas, *wallets* no declaradas, transacciones pendientes, errores de importación de datos o movimientos no autorizados.

5.3.5 La función del TxID como elemento de trazabilidad

El identificador de transacción o *transaction hash* (TxID) constituye uno de los principales elementos técnicos para conectar la contabilidad con la *blockchain*. Sin embargo, el TxID no sustituye toda la documentación contable. Su función consiste en acreditar determinadas características de una operación registrada en una *blockchain* (direcciones participantes, cantidades, momento de incorporación, comisiones y estado de la transacción).

Sin embargo, **no demuestra por sí mismo**:

- Quién es el propietario económico de cada dirección.
- Cuál fue la causa jurídica de la transferencia.
- Qué contrato la originó.
- Cuál es su clasificación contable.

Por esta razón, la evidencia *on-chain* debe integrarse imperativamente con la evidencia *off-chain*. El GAFI reconoce también la importancia de información relativa al originador y beneficiario dentro del régimen regulatorio aplicable a proveedores de servicios de activos virtuales, especialmente mediante los requerimientos asociados con la denominada *Travel Rule* (GAFI, 2021).

5.3.6 Evidencia *on-chain* y *off-chain*

Para efectos de auditoría y peritaje contable, resulta útil dividir las fuentes de evidencia en dos grupos:

Evidencia *on-chain*	Evidencia *off-chain*
Dirección *blockchain*	Estados de cuenta bancarios
TxID	Contratos
Bloque	Comprobantes
Timestamp	Facturas
Cantidad transferida	Extractos de *exchanges*
Comisión de red	Información KYC
Dirección origen/destino	Correos y confirmaciones
Smart contract	Registros internos
Token contract	Libros contables

Una conclusión robusta requiere correlacionar ambos grupos. La *blockchain* puede demostrar que una determinada cantidad fue transferida de una

dirección hacia otra, pero para determinar el tratamiento contable es necesario establecer quién controlaba las direcciones y cuál fue la sustancia económica de la operación.

5.3.7 Separación entre *wallets* empresariales y personales

Una debilidad particularmente relevante desde la perspectiva de control interno consiste en utilizar una misma *wallet* para operaciones personales y empresariales. Esta práctica dificulta determinar:

- Qué activos pertenecen efectivamente a la entidad.
- Qué transferencias corresponden al negocio.
- Cuáles constituyen aportes o retiros de propietarios.
- Cuáles representan gastos personales.
- Qué costo corresponde a cada activo y qué saldos deben incluirse en los estados financieros.

En consecuencia, una política adecuada debería procurar la segregación entre *wallets* empresariales y personales, así como la identificación formal de las personas autorizadas para iniciar y aprobar movimientos. En investigaciones forenses, la utilización conjunta de *wallets* exige reconstruir cada operación individualmente antes de atribuir el saldo completo a una persona o entidad.

5.3.8 Matriz general de registro de operaciones

Las principales operaciones pueden sintetizarse del siguiente modo:

Operación	Débito principal	Crédito principal	Consideración especial
Compra con moneda fiduciaria	Criptoactivo	Banco	Determinar clasificación y costo
Venta de intangible	Banco	Criptoactivo + ganancia, o reconocimiento de pérdida	Ganancia no presentada como ingreso ordinario bajo NIC 38
Venta de inventario	Banco/CxC y costo de venta	Ingreso e inventario	NIC 2 + norma de ingresos correspondiente
Recepción por venta de bienes/servicios	Criptoactivo	Ingreso	Contraprestación no monetaria
Pago de obligación con cripto	Pasivo	Criptoactivo ± resultado	Existe disposición del criptoactivo

Operación	Débito principal	Crédito principal	Consideración especial
Intercambio cripto-cripto	Nuevo criptoactivo	Criptoactivo entregado ± resultado	No requiere moneda fiduciaria para producir efecto contable
Transferencia entre wallets propias	Movimiento auxiliar	Movimiento auxiliar	Normalmente no genera disposición
Comisión pagada en cripto	Costo/gasto según naturaleza	Criptoactivo	Analizar disposición de las unidades utilizadas
Deterioro	Pérdida	Deterioro/activo	Aplicar NIC 36 cuando corresponda
Revaluación válida	Criptoactivo	ORI/superávit, según corresponda	Requiere condiciones de NIC 38
Broker-trader	Activo o pérdida	Ganancia o activo	Valor razonable menos costos de venta
Minería	Según política desarrollada	Según naturaleza económica	No existe tratamiento NIIF único específico
Staking	Según política y sustancia	Según naturaleza económica	Diferenciar protocolo propio de servicio a clientes
Airdrop/fork	Evaluación bajo NIC 8	Evaluación bajo NIC 8	No reconocer automáticamente como ingreso
Operaciones DeFi	Según derechos obtenidos	Según derechos entregados	Analizar sustancia contractual

5.3.9 Riesgos de incorrección en el registro

Desde una perspectiva contable y forense, existen determinadas situaciones que deberían generar procedimientos adicionales de revisión:

- Operaciones sin documentación diferente del registro *blockchain*.
- Compras registradas sin salida correlacionada de fondos.
- Transferencias a *wallets* de terceros presentadas como movimientos internos.
- Operaciones cripto-a-cripto omitidas o registros duplicados entre *exchanges* y *blockchain*.
- Utilización indiscriminada del precio de mercado como costo histórico.
- Comisiones no contabilizadas y diferencias entre saldos contables y *wallets*.
- Utilización de *wallets* personales para operaciones corporativas.
- Operaciones registradas con fecha diferente a la real por errores de zona horaria.
- Modificación retroactiva de costos.
- Activos mantenidos en *exchanges* que no aparecen en los registros contables.

Estos indicadores no constituyen por sí mismos evidencia de fraude; representan señales de riesgo que requieren explicación, documentación y procedimientos adicionales.

5.3.10 Propuesta de trazabilidad contable-forense

Para los propósitos de este Manual, puede emplearse una matriz de trazabilidad que conecte cada asiento con su evidencia tecnológica y financiera:

Nivel	Evidencia que debe identificarse
1. Hecho económico	Compra, venta, pago, intercambio, recompensa, etc.
2. Contraparte	Persona, empresa, *exchange*, protocolo
3. Medio de pago	Banco, *wallet*, otro criptoactivo
4. Evidencia blockchain	TxID, dirección, bloque, *timestamp*
5. Evidencia externa	Factura, contrato, *exchange*, comprobante
6. Clasificación NIIF	NIC 38, NIC 2, NIIF 9 u otra
7. Medición	Costo, VNR, valor razonable, etc.
8. Asiento	Debe / Haber
9. Libro auxiliar	Unidades y costo
10. Libro mayor	Importe en moneda funcional
11. Estados financieros	Presentación y revelación

La aplicación de esta metodología permite construir una cadena de trazabilidad contable que conecta el hecho económico original con el importe presentado finalmente en los estados financieros.

5.3.11 Caso integral de registro

Supóngase que una entidad cuya moneda funcional se expresa en unidades monetarias realiza las siguientes operaciones:

- Compra 2 BTC por 80,000 u.m.
- Transfiere ambos BTC desde el *exchange* a una *wallet* propia.
- Utiliza 0.50 BTC para pagar una obligación de 30,000 u.m.
- Intercambia 0.50 BTC por ETH.
- Mantiene 1 BTC al cierre.

La metodología correcta no consiste en comparar únicamente el dinero inicialmente invertido con el valor final de la *wallet*. Cada operación debe reconstruirse separadamente:

La compra constituye el reconocimiento inicial de los 2 BTC.

La transferencia del *exchange* hacia una *wallet* propia no necesariamente constituye una nueva adquisición, ya que puede tratarse únicamente de un cambio de custodia.

El pago de una obligación con 0.50 BTC implica la baja de esa fracción del criptoactivo y la extinción de la cuenta por pagar, generándose el resultado por disposición que corresponda.

El intercambio de 0.50 BTC por ETH constituye una operación económicamente diferente y, en el supuesto de aplicación de la NIC 38, deberá analizarse conforme a los requisitos relativos al intercambio de activos no monetarios.

Finalmente, el BTC restante deberá conservar su costo atribuible y recibir al cierre el tratamiento de medición posterior establecido por la política aplicable.

Este caso evidencia que el análisis basado exclusivamente en comparar el saldo bancario inicial frente al saldo bancario final sería insuficiente para reconstruir las operaciones con activos virtuales.

5.3.12 Registro y cadena de custodia de la evidencia digital

En auditorías forenses y peritajes, el soporte del asiento contable debe conservarse de forma que permita comprobar su autenticidad, integridad y relación con la operación examinada. La evidencia *blockchain* posee características de inmutabilidad en el registro distribuido, pero los documentos adicionales utilizados para atribuir una *wallet*, identificar una contraparte o demostrar una operación pueden proceder de sistemas internos, *exchanges*, dispositivos electrónicos o archivos exportados.

Por ello, resulta recomendable documentar la fuente de obtención, fecha de extracción, responsable, formato original y procedimientos utilizados para preservar la información. La NIA 500 establece el principio general de obtener evidencia de auditoría suficiente y adecuada y evaluar la fiabilidad de la información utilizada como evidencia (IAASB, vigente). En consecuencia, una captura de pantalla aislada de un saldo de criptomonedas debería evaluarse con cautela cuando resulte posible obtener evidencia más robusta mediante estados de cuenta, exportaciones del *exchange*, verificación *blockchain* o confirmaciones externas.

5.3.13 Registro contable y prevención del lavado de activos

Aunque el registro contable y la prevención del lavado de activos persiguen objetivos diferentes, las operaciones con activos virtuales generan un espacio significativo de convergencia entre ambas disciplinas. El GAFI exige que los países sometan a los proveedores de servicios de activos virtuales (VASP) a medidas relevantes de prevención, incluyendo requerimientos de identificación, supervisión y transferencia de información (GAFI, 2021).

Desde la perspectiva pericial, la documentación contable puede contribuir a responder preguntas clave:

1. ¿De dónde provino el dinero utilizado para adquirir los criptoactivos?
2. ¿Quién controlaba la *wallet*?
3. ¿Cuándo se adquirieron y qué contraparte intervino?
4. ¿A qué dirección fueron transferidos y qué activo se recibió a cambio?
5. ¿Cómo se determinó su valor y dónde quedó registrado el resultado económico?

Estas preguntas permiten vincular el análisis contable con la trazabilidad financiera y patrimonial. No obstante, la existencia de múltiples transferencias, utilización de varias *wallets* o participación en protocolos descentralizados no constituye por sí misma prueba de actividad ilícita; la conclusión pericial debe sustentarse en evidencia objetiva y en el análisis integral de las operaciones.

5.3.14 Política contable para el registro de operaciones con criptoactivos

Las entidades que efectúen operaciones materiales con criptomonedas deberían desarrollar una política contable específica que permita aplicar criterios homogéneos. La NIC 8 exige consistencia en la aplicación de políticas contables a transacciones, eventos y condiciones similares, salvo que una NIIF requiera o permita categorizaciones diferentes (IFRS Foundation, 2021, NIC 8).

Una política técnicamente estructurada debería definir:

- La clasificación de cada categoría de criptoactivo.
- El momento de reconocimiento y baja.
- La metodología para determinar el costo y la fórmula de asignación.
- El tratamiento de comisiones, operaciones cripto-a-cripto y transferencias internas.
- El tratamiento de minería, *staking*, *airdrops* y operaciones DeFi.

- La conversión a moneda funcional, conciliaciones, controles sobre *wallets* y documentación de respaldo.

La existencia de una política formal reduce el riesgo de seleccionar tratamientos distintos para operaciones económicamente semejantes con el propósito de modificar los resultados del período.

5.3.15 Criterio integrador para el registro de operaciones con criptomonedas

El registro contable de operaciones con criptomonedas debe fundamentarse en la sustancia económica de cada transacción, y no exclusivamente en su manifestación tecnológica. La *blockchain* constituye una fuente extraordinariamente relevante de información sobre determinadas transferencias, pero la existencia de un movimiento entre direcciones no determina por sí misma su clasificación contable.

Para las criptomonedas comprendidas en la decisión del IFRS Interpretations Committee, la contabilización debe partir de su clasificación conforme a la NIC 2 o la NIC 38 (IFRS Interpretations Committee, 2019). Para otros criptoactivos que incorporen derechos contractuales deberá analizarse, entre otras normas, la NIIF 9. Cuando la operación carezca de un tratamiento específicamente prescrito por las NIIF, deberá aplicarse el juicio profesional siguiendo la jerarquía prevista por la NIC 8 (IFRS Foundation, s. f.).

Desde una perspectiva de auditoría forense, un registro contable adecuado debe permitir recorrer la operación en ambos sentidos:

Hecho económico → documentación → blockchain/exchange → medición → asiento → libro mayor → estados financieros

y, posteriormente, en sentido inverso:

Estados financieros → libro mayor → asiento → documentación → blockchain/exchange → contraparte → origen y destino económico

Esta trazabilidad bidireccional constituye un elemento fundamental para verificar la integridad, exactitud y razonabilidad del registro de operaciones con criptoactivos, identificar operaciones omitidas o duplicadas y reconstruir movimientos patrimoniales dentro de investigaciones financieras.

5.4 Autonomía entre el tratamiento contable y el tratamiento tributario

5.4.1 Tratamiento contable y tributario

Uno de los principios fundamentales para el análisis de los criptoactivos consiste en diferenciar la base contable de la base tributaria.

- **La contabilidad financiera** persigue proporcionar información útil sobre la situación financiera y el desempeño económico de una entidad conforme a las NIIF.
- **El sistema tributario**, en cambio, determina obligaciones fiscales conforme a la legislación de cada jurisdicción.

Por tanto, pueden existir divergencias permanentes o temporarias entre:

importe en libroscosto fiscalvalor de mercado

Por ejemplo, un criptoactivo podría encontrarse registrado contablemente bajo un modelo de costo o revaluación, mientras que la legislación fiscal podría reconocer la renta únicamente al momento de su disposición. También puede suceder lo contrario: determinadas jurisdicciones establecen reglas fiscales específicas que no coinciden con el reconocimiento contable.

Esta distinción tiene consecuencias directas en la determinación del impuesto corriente y, cuando resulte aplicable, de los impuestos diferidos conforme a la NIC 12. La OCDE ha documentado importantes diferencias entre países respecto del momento y la naturaleza de la imposición de las monedas virtuales, especialmente en relación con la minería, la compraventa, los intercambios y la disposición de estos activos (OCDE, 2020).

5.4.2 Determinación de la naturaleza fiscal del criptoactivo

Antes de determinar el impuesto aplicable, debe identificarse cómo califica el ordenamiento tributario el activo involucrado. Dependiendo de la jurisdicción, la aproximación normativa puede encuadrarlo como:

- Activo intangible
- Propiedad o bien mueble
- Activo financiero
- *Commodity* (mercancía)
- Activo de inversión
- Instrumento de pago

- Una categoría tributaria específica de nueva creación

La OCDE comprobó en su estudio comparado que existen divergencias importantes en este aspecto, y que muy pocas jurisdicciones calificaban las monedas virtuales simplemente como moneda de curso legal para efectos tributarios (OCDE, 2020).

La calificación posee consecuencias prácticas directas: si el criptoactivo es considerado un activo patrimonial, su disposición puede quedar sometida a reglas de ganancias de capital; si constituye inventario o activo de negociación dentro de una actividad empresarial, los resultados se calificarán como renta ordinaria de negocio; y si el *token* representa jurídicamente deuda, participación societaria u otro derecho contractual, resultarán aplicables las disposiciones del instrumento subyacente. En consecuencia:

La denominación tecnológica del activo no determina automáticamente su tratamiento tributario.

5.4.3 Identificación del hecho imponible

Uno de los principales desafíos consiste en establecer qué acontecimientos relacionados con criptoactivos generan consecuencias tributarias. La siguiente matriz resume las principales operaciones y su cuestión tributaria central:

Operación	Cuestión tributaria principal
Compra con moneda fiduciaria	Determinación del costo fiscal inicial.
Venta por moneda fiduciaria	Ganancia o pérdida realizada.
Intercambio cripto-cripto	Posible disposición de un activo y adquisición de otro.
Pago de bienes con cripto	Posible disposición del criptoactivo + tributación del bien.
Pago de servicios con cripto	Posible disposición + tributación del servicio.
Recepción como remuneración	Renta del receptor y costo fiscal inicial.
Minería	Momento y naturaleza de la renta.
Staking	Tratamiento de las recompensas.
Airdrop	Momento de reconocimiento.
Hard fork	Existencia y momento de renta.
DeFi	Análisis de cada derecho transferido o recibido.
Donación	Posible impuesto sobre donaciones y/o disposición.
Herencia	Impuesto sucesorio donde exista.
Robo o pérdida	Deducibilidad o reconocimiento de pérdida.
NFT	Tributación según su naturaleza y operación.

Operación	Cuestión tributaria principal
Tokenización	Aplicación de las reglas del activo subyacente.

La OCDE identifica precisamente la creación, el intercambio, la utilización, la donación, la herencia, la pérdida, el robo y fenómenos como los *hard forks*, las *stablecoins* y los *tokens* generadores de rendimiento como las materias respecto de las cuales las administraciones tributarias necesitan reglas suficientemente claras (OCDE, 2020).

5.4.4 Adquisición de criptomonedas mediante moneda fiduciaria

La simple adquisición de un criptoactivo mediante moneda fiduciaria requiere, como mínimo, determinar su costo fiscal inicial. Supóngase:

Compra: 1 BTC = 40,000 u.m.

Costos fiscalmente incorporables (comisiones, *gas fees*): 400 u.m.

$$\text{Costo fiscal potencial} = 40,000 + 400 = 40,400 \text{ u.m.}$$

Sin embargo, la incorporación efectiva de comisiones u honorarios dependerá de la legislación local. En este momento puede no existir todavía una ganancia económica realizada, pero se origina información indispensable para determinar posteriormente el resultado fiscal. Por ello, una adecuada documentación debería conservar:

$$\text{fecha} + \text{cantidad} + \text{precio} + \text{comisión} + \text{moneda de pago} + \text{tipo de cambio} + \text{fuente del precio} + \text{comprobante} + \text{TxID / exchange}$$

La insuficiencia documental en la fecha de adquisición producirá posteriormente importantes dificultades para acreditar el costo fiscal ante el fisco.

5.4.5 Venta de criptomonedas por moneda fiduciaria

La conversión de un criptoactivo a moneda fiduciaria constituye uno de los supuestos más evidentes de realización fiscal. De forma conceptual:

Ganancia fiscal} = Valor de disposición -Costo fiscal atribuible}$$

Por ejemplo:

Costo fiscal: 40,000 u.m.

Precio de venta: 65,000 u.m.

Costos deducibles de disposición: 1,000 u.m.

Resultado = 65,000 - 1,000 - 40,000 = 24,000 u.m.

Dependiendo de la jurisdicción y las circunstancias del contribuyente, esta ganancia podrá clasificarse como ganancia de capital, renta empresarial, renta ordinaria o renta especulativa (OCDE, 2020).

5.4.6 Intercambio cripto-cripto

Una de las cuestiones tributarias más relevantes ocurre cuando no interviene dinero fiduciario, como por ejemplo en operaciones del tipo BTC ETH o ETH USDC. Desde un punto de vista económico y fiscal, existe una disposición de un activo y la adquisición de otro.

El cálculo conceptual de la ganancia realizada se expresa como:

$$\text{Ganancia} = \text{Valor de mercado del activo entregado} - \text{Costo fiscal del activo entregado}$$

Por ejemplo:

Costo fiscal de 1 BTC: 30,000 u.m.

Valor de mercado al intercambiarlo por ETH: 50,000 u.m.

Potencial ganancia realizada: $50,000 - 30,000 = 20,000 \text{ u.m.}$

Simultáneamente, las 50,000 u.m. se convierten en la base inicial del ETH recibido, sujeto a las normas domésticas. No obstante, este tratamiento no constituye una regla universal, ya que algunas legislaciones pueden admitir diferimientos, exenciones o reglas de *rollover*.

5.4.7 Diferencia entre "operación reportable" y "operación gravada"

Esta distinción adquiere máxima relevancia con la implementación del *Crypto-Asset Reporting Framework* (CARF) de la OCDE. El CARF considera objeto de reporte los intercambios entre criptoactivos y monedas fiduciarias, los intercambios entre diferentes criptoactivos y determinadas transferencias (OCDE, 2023). Sin embargo:

Que una operación deba ser reportada bajo CARF no significa que necesariamente esté gravada.

El CARF constituye fundamentalmente un estándar de transparencia e intercambio automático de información tributaria. La determinación del impuesto continúa dependiendo estrictamente de la legislación fiscal sustantiva de cada jurisdicción, evitando confundir la obligación de informar con la obligación de pagar un tributo.

5.4.8 Pago de bienes o servicios mediante criptomonedas

Cuando un contribuyente utiliza criptomonedas para adquirir bienes o servicios, coexisten dos hechos tributarios diferenciados:

Operación del vendedor: Realiza una operación ordinaria (entrega del bien/servicio a cambio de una contraprestación), cuya naturaleza fiscal no se altera por efectuarse en criptoactivos.

Operación del comprador: Está disponiendo de un activo cuyo valor fiscal difiere del valor de mercado utilizado para pagar.

Por ejemplo:

Costo fiscal del criptoactivo entregado: 3,000 u.m.

Valor del bien adquirido: 5,000 u.m.

Ganancia realizada en el criptoactivo: $5,000 - 3,000 = 2,000 u.m.

Por tanto, pagar con criptomonedas no equivale fiscalmente a pagar con efectivo; puede detonar la realización de una ganancia sobre el activo entregado (OCDE, 2023).

5.4.9 Recepción de criptomonedas por venta de bienes o prestación de servicios

Cuando una empresa o profesional recibe criptoactivos como contraprestación, deben separarse dos momentos:

a) El ingreso ordinario originado por el bien o servicio prestado (ej. 10,000 u.m.), el cual fija el costo fiscal inicial del BTC recibido.

b) Las consecuencias tributarias posteriores del criptoactivo.

Si el BTC recibido por 10,000 u.m. se vende posteriormente por 14,000 u.m.:

Resultado por disposición= 14,000 - 10,000 = 4,000 u.m.

Estas 4,000 u.m. corresponden a la variación patrimonial del activo, no al servicio original.

5.4.10 Remuneraciones pagadas mediante criptomonedas

Cuando una entidad paga remuneraciones a trabajadores o proveedores con activos virtuales, se evalúa:

Para quien recibe: Reconocimiento de renta por trabajo o servicios.

Para quien paga: Eventual disposición del criptoactivo y reconocimiento del gasto laboral o profesional.

Por ejemplo, ante una remuneración de 5,000 u.m. cubierta con un criptoactivo cuyo costo fiscal era de 3,500 u.m., se produce simultáneamente el gasto de 5,000 u.m., la baja del criptoactivo y un resultado fiscal por su disposición de 1,500 u.m., sin perjuicio de las obligaciones de retención y seguridad social aplicables.

5.4.11 Tributación de la minería

La minería presenta dos momentos críticos: la recepción de la recompensa y la posterior disposición del criptoactivo. Algunas jurisdicciones gravan la obtención de los tokens cuando la actividad tiene carácter empresarial; otras difieren el gravamen hasta su enajenación (OCDE, 2020). Deben evaluarse analíticamente:

Recompensa de bloque y comisiones de transacción.

Costos operativos (electricidad, infraestructura, depreciación de equipos).

Participación en *mining pools* y el momento exacto en que se adquiere el control jurídico y económico de los tokens.

5.4.12 *Staking* y recompensas de validación

El *staking* plantea desafíos similares al requerir determinar la existencia de actividad empresarial, la disponibilidad económica de la recompensa, su valor de mercado inicial y el costo fiscal asignable al activo recibido. El CARF contempla clasificar estos ingresos cuando el proveedor posea la información correspondiente, constituyendo un estándar de reporte y no una regla uniforme de causación fiscal (OCDE, 2023).

5.4.13 *Airdrops*

Los *airdrops* (distribuciones gratuitas o promocionales de *tokens*) no responden a una regla homogénea. Las alternativas conceptuales adoptadas por las legislaciones comparadas comprenden:

- Tributación inmediata al recibir el *token*.
- Diferimiento del gravamen hasta su disposición final.

- Tratamiento diferenciado según la existencia o no de una actividad previa del usuario (OCDE, 2020).

Por tanto, no es técnicamente correcto asumir que todo *airdrop* constituye renta automática al momento de su recepción.

5.4.14 *Hard forks*

Un *hard fork* genera una nueva cadena y unidades asociadas. La divergencia fiscal radica en determinar si la mera aparición de las nuevas unidades constituye renta gravada y cuál es su costo fiscal inicial (que en algunas jurisdicciones se fija en cero o se deriva del activo original), condicionado además a la disponibilidad técnica efectiva del contribuyente sobre los nuevos activos (OCDE, 2020).

5.4.15 Finanzas descentralizadas (DeFi)

Las operaciones DeFi (*yield farming*, provisión de liquidez, *liquidity provider tokens*, préstamos y *wrapped tokens*) exigen responder a una premisa fundamental antes de aplicar un tratamiento fiscal:

$$\text{¿Qué derecho económico entregó el contribuyente y qué derecho recibió a cambio?}$$

Si no existió transferencia sustancial de control o disposición económica, la operación no debe asimilarse automáticamente a una venta o permuta (OCDE, 2023).

5.4.16 *Stablecoins*

La estabilidad nominal de una *stablecoin* (como USDC) no elimina su relevancia tributaria. Operaciones del tipo $\text{USDC} \rightarrow \text{BTC}$ representan fiscalmente un intercambio de activos. Aunque la ganancia sobre la *stablecoin* pueda ser nula o marginal por mantener paridad con la moneda fiduciaria, la transacción conserva plena vigencia para propósitos de reporte, registro e información bajo marcos como el CARF (OCDE, 2023).

5.4.17 NFTs y activos del mundo real tokenizados

NFTs: Exigen examinar tanto el soporte digital como los derechos subyacentes asociados (arte, licencias, propiedad intelectual o derechos de ingreso), distinguiendo el tratamiento para el creador, la primera venta, las regalías y las sucesivas reventas.

Activos tokenizados: La tecnología de representación no desplaza la naturaleza del activo subyacente. Un *token* de deuda, de acciones o inmobiliario se somete estrictamente a las reglas tributarias de la figura jurídica o financiera subyacente.

5.4.18 Determinación del costo fiscal

Ante adquisiciones sucesivas a distintos precios (ej. compras de BTC en enero a 20,000 u.m., en marzo a 30,000 u.m. y en junio a 50,000 u.m.), la enajenación posterior de unidades exige aplicar un método de costeo fiscal aceptado por la ley local, tales como:

- Identificación específica
- FIFO (*First-In, First-Out*)
- Costo promedio ponderado
- Sistemas de agrupación o *pooling*

La existencia de trazabilidad *blockchain* no faculta al contribuyente para elegir arbitrariamente el lote fiscal que minimice su carga tributaria, debiendo aplicar consistentemente la regla de valoración prescrita por la autoridad fiscal (OCDE, 2020)s.

5.4.19 Valoración tributaria

Para determinar la renta o ganancia gravada, resulta indispensable expresar el criptoactivo en moneda fiduciaria, lo cual plantea desafíos operativos inmediatos:

1. ¿Qué *exchange* o fuente de precios utilizar?
2. ¿Qué hora y zona horaria considerar?
3. ¿Aplicar precio *spot*, promedio ponderado, mercado local o referencia internacional?
4. ¿Cómo proceder ante diferencias sustanciales entre plataformas o frente a activos carentes de un mercado líquido?

La volatilidad y fragmentación del mercado dificultan la valoración y generan importantes cargas de cumplimiento (OCDE, 2020; Baer et al., 2023). Por ello, una política fiscal adecuadamente documentada debe permitir reconstruir de forma inequívoca la traza de valoración:

- activounidadesfecha/horafuentecotizaciónmonedatipo de cambiovalor fiscal
- La consistencia metodológica es indispensable para impedir la selección oportunista de precios por parte del contribuyente.

5.4.20 Ganancias no realizadas

Es imperativo distinguir conceptualmente entre la apreciación económica (plusvalía latente) y la renta fiscal realizada o reconocida. Supóngase:

- Costo de adquisición: 20,000 u.m.
- Valor de mercado al cierre del período: 70,000 u.m.
- Estado del activo: No enajenado.

A pesar de existir una apreciación económica de 50,000 u.m., la tributación dependerá estrictamente de si la legislación local aplica un criterio estricto de realización (disposición) o un sistema de valoración periódica a valor de mercado (*mark-to-market*). Por tanto:

$$\text{ganancia contable} \neq \text{ganancia tributaria necesariamente}$$

De igual forma, una pérdida de valor reconocida contablemente por deterioro no debe considerarse automáticamente deducible para efectos tributarios si la norma fiscal exige la realización efectiva del menoscabo patrimonial.

5.4.21 Pérdidas tributarias

La caída de precios, la venta con pérdida, el fraude, el robo o la pérdida de acceso a las claves privadas (*lost keys*) pueden detonar consecuencias fiscales muy diversas. Debe analizarse rigurosamente:

- La naturaleza de la pérdida y su carácter realizado o no realizado.
- La robustez de la documentación probatoria.
- Las limitaciones legales de compensación y la posibilidad de arrastre de pérdidas (*carryforward*).
- La existencia de coberturas de seguros o posibilidades de recuperación posterior.

La OCDE identifica expresamente las pérdidas y robos de monedas virtuales como materias que requieren orientación tributaria clara (OCDE, 2020). En

sede forense, resulta especialmente crítico evitar que una supuesta pérdida de claves sea invocada sin la trazabilidad técnica suficiente para justificar una minoración patrimonial o una deducción fiscal.

5.4.22 Tributación indirecta: IVA, IGV o GST

Los impuestos al consumo representan un ámbito fundamental. El estudio comparado de la OCDE evidenció mayor convergencia internacional en el tratamiento del IVA que en el impuesto sobre la renta: en numerosas jurisdicciones, el mero intercambio de monedas virtuales por moneda fiduciaria u otras monedas virtuales no queda gravado con IVA de la misma forma que una venta ordinaria de bienes (OCDE, 2020).

No obstante, cuando se utiliza un criptoactivo para adquirir un producto, coexisten dos hechos económicos:

El criptoactivo utilizado como pago: Se rige por el tratamiento propio de los instrumentos de pago o divisas exentas según la jurisdicción.

El bien o servicio adquirido: Mantiene su afectación plena al impuesto al consumo conforme a las reglas ordinarias.

5.4.23 El caso *Hedqvist* en la Unión Europea

Un precedente jurisprudencial de gran relevancia es la sentencia del Tribunal de Justicia de la Unión Europea (TJUE) del 22 de octubre de 2015 en el asunto C-264/14 (*Skatteverket v. David Hedqvist*).

El Tribunal determinó que los servicios de intercambio entre Bitcoin y monedas tradicionales quedaban comprendidos dentro de la exención del IVA aplicable a las operaciones relativas a divisas (TJUE, 2015), contribuyendo a evitar una doble imposición económica por vía del IVA. Sin embargo, esta doctrina responde estrictamente al derecho comunitario europeo y no constituye una regla de aplicación automática en terceros países.

5.4.24 Impuestos patrimoniales, sucesorios y sobre donaciones

Cuando los criptoactivos son calificados jurídicamente como propiedad o bienes muebles, pueden quedar sujetos —dependiendo de la legislación de cada Estado a:

- Impuestos sobre el patrimonio o la riqueza.
- Impuestos sucesorios (herencias).
- Impuestos sobre donaciones y transferencias gratuitas (OCDE, 2020).

Estas figuras impositivas plantean desafíos operativos complejos relacionados con la valoración a la fecha de devengo (fallecimiento o donación) y con la prueba de titularidad sobre activos custodiados mediante claves privadas.

5.4.25 Residencia fiscal

La naturaleza descentralizada y global de los criptoactivos no desplaza las reglas tradicionales de sujeción por residencia. Una operativa típica puede involucrar múltiples jurisdicciones:

Residente en País AUso de exchange en País BTenencia en blockchainVenta a sujeto en País CFONDOS en cuenta de País D

Ante este escenario, la pregunta tributaria inicial no debe ser *"¿dónde está la blockchain?"*, sino:

"¿Qué jurisdicción posee potestad tributaria conforme a su legislación interna y a los convenios para evitar la doble imposición aplicables?"

La residencia del contribuyente continúa siendo el eje rector en los sistemas que gravan la renta mundial (*worldwide income*).

5.4.26 Fuente de la renta

En un ecosistema *blockchain* distribuido globalmente, la aplicación de los criterios tradicionales de fuente (como la ubicación física de los servidores, los nodos validadores o el lugar de desarrollo de la actividad) carece de relevancia práctica. Por tanto, la atribución de la fuente de la renta debe determinarse de manera armónica conforme a las normas domésticas de sujeción y los convenios internacionales vigentes.

5.4.27 Convenios para evitar la doble imposición

Las operaciones transfronterizas con criptoactivos generan frecuentes conflictos de potestad tributaria. El Modelo de Convenio Tributario de la OCDE (2019) busca resolver la doble imposición jurídica, exigiendo una prelación lógica ineludible:

$$\text{Caracterización jurídica de la renta} \longrightarrow \text{Identificación del artículo aplicable del convenio}$$

No existe en los convenios bilaterales un artículo universal denominado "rentas de criptoactivos"; su calificación bajo categorías convencionales (beneficios empresariales, ganancias de capital, intereses o regalías) dependerá de la naturaleza económica y jurídica del token, requiriendo verificar los criterios normativos específicos adoptados por cada administración tributaria nacional.

5.4.28 Establecimiento permanente y actividades empresariales

Cuando entidades dedicadas a la intermediación (*exchanges*, custodios, operadores de cajeros automáticos, proveedores institucionales o mineros) operan a escala transfronteriza, debe evaluarse la existencia de un establecimiento permanente conforme al artículo 7 del Modelo OCDE (2019). No obstante, la mera ubicación de servidores, *smart contracts* o infraestructura descentralizada en un territorio no debe equipararse de forma automática a la configuración de un establecimiento permanente sin cumplir los requisitos materiales del convenio aplicable.

5.4.29 Precios de transferencia

Las transacciones con criptoactivos entre partes vinculadas (por ejemplo, la transferencia de tokens entre una sociedad matriz y una subsidiaria) plantean exigencias rigurosas de precios de transferencia. El análisis debe fundamentarse estrictamente en el principio de plena competencia (*arm's length principle*), examinando:

La naturaleza económica del token y su valor de mercado.

Las funciones desempeñadas, los riesgos asumidos y los activos utilizados por cada parte.

La existencia de comparables fiables, especialmente compleja en mercados ilíquidos o en tokens de emisión propia del grupo empresarial.

5.4.30 Fiscalidad de operaciones transfronterizas

Una auditoría o análisis de una transacción internacional exige reconstruir de forma secuencial los siguientes eslabones:

- residenciacontraparteintermediarionaturaleza de la rentafuenteconvenioimpuesto satisfechocrédito fiscal

Operar a través de un *exchange* extranjero no convierte automáticamente la renta en fuente extranjera, del mismo modo que mantener activos en una billetera de autocustodia (*self-hosted wallet*) no exime de tributación bajo la ficción de que el activo "no se encuentra en ninguna jurisdicción".

5.4.31 Riesgo de doble imposición

Las asimetrías de calificación entre Estados (por ejemplo, que el Estado A considere la operación una ganancia de capital y el Estado B una renta empresarial) generan riesgos severos de doble imposición jurídica y económica, divergencias en el momento de reconocimiento y controversias en la aplicación de créditos fiscales, subrayando la necesidad de conservar un soporte probatorio impecable.

5.4.32 De la pseudonimidad a la transparencia tributaria global

Históricamente, el Estándar Común de Reporte (*Common Reporting Standard* -CRS) permitió a las administraciones fiscalizar cuentas financieras tradicionales, pero dejó un vacío normativo frente a los criptoactivos operados mediante intermediarios no tradicionales o billeteras privadas (OCDE, 2023). Para cerrar esta brecha de información, la OCDE impulsó un cambio estructural hacia la transparencia global.

5.4.33 Crypto-Asset Reporting Framework (CARF)

El marco CARF (*Crypto-Asset Reporting Framework*), desarrollado por la OCDE, establece un estándar global para el intercambio automático, estandarizado y anual de información tributaria sobre criptoactivos (OCDE, 2023). Se compone de tres pilares normativos:

Reglas modelo para la legislación interna.

Acuerdos multilaterales de autoridades competentes (CARF MCAA).

Formatos electrónicos estandarizados para la transmisión de datos.

5.4.34 Cuatro componentes sustantivos del CARF

Las reglas del CARF se estructuran en torno a cuatro ejes fundamentales que facilitan la labor de fiscalización y auditoría forense:

Activos comprendidos (*Relevant Crypto-Assets*).

Entidades obligadas a recopilar y reportar (*Reporting Crypto-Asset Service Providers*).

Transacciones objeto de reporte (operaciones cruzadas y transferencias).

Procedimientos de diligencia debida para la identificación de usuarios y su residencia fiscal (OCDE, 2023).

5.4.35 Activos comprendidos bajo CARF

El marco abarca criptoactivos transferibles, *stablecoins*, derivados emitidos como criptoactivos y determinados NFTs con finalidad de inversión o pago. Se excluyen expresamente aquellos activos sin funcionalidad de inversión o pago, las monedas digitales de bancos centrales (CBDC) y los productos de dinero electrónico ya cubiertos por el CRS (OCDE, 2023), evidenciando la distancia entre los conceptos tributarios de reporte y las clasificaciones contables NIIF.

5.4.36 Proveedores de servicios obligados a reportar

Los **RCASP** (*Reporting Crypto-Asset Service Providers*) comprenden a las entidades que facilitan transacciones de intercambio de criptoactivos por cuenta de clientes (*exchanges*, corredores, *dealers* y cajeros automáticos), vinculando de forma unívoca la identidad del usuario con la operación y el volumen transado (OCDE, 2023).

5.4.37 Operaciones reportables bajo CARF

El estándar exige reportar de forma estandarizada los siguientes bloques operacionales:

Tipo de operación	Estatus bajo CARF
Criptoactivo ↔ Moneda fiduciaria	Reportable (expresado en valor fiduciario)

Tipo de operación	Estatus bajo CARF
Criptoactivo ↔ Criptoactivo	Reportable (disposición del activo A y adquisición del activo B)
Determinadas transferencias	Reportable (incluyendo categorización cuando sea posible)

Fuente: (OCDE, 2023).

5.4.38 Transferencias hacia wallets de autocustodia

El CARF presta especial atención a las transferencias enviadas desde proveedores regulados hacia billeteras de autocustodia (*self-hosted wallets*). Aunque estas salidas generan alertas de riesgo fiscal, la norma contempla esquemas de agregación e intercambio adicional, demostrando que la autocustodia no equivale a invisibilidad tributaria (OCDE, 2023), constituyendo para el auditor forense un punto de partida crítico para reconstruir la cadena *on-chain*.

5.4.39 Diligencia debida y residencia tributaria bajo CARF

Mediante procedimientos de autocertificación alineados con los estándares de debida diligencia de clientes (KYC/AML) y las directrices del CRS, el CARF vincula de manera permanente la identidad civil, la residencia fiscal, la operativa transaccional y la traza en la cadena de bloques (OCDE, 2023).

5.4.40 CARF y Common Reporting Standard (CRS)

El CARF y el CRS operan de manera complementaria y no excluyente. Mientras el CARF regula la tenencia directa y operativa de criptoactivos, las modificaciones introducidas al CRS cubren las exposiciones indirectas a través de vehículos de inversión financiera tradicional, ampliando de forma integral el perímetro de control de las administraciones tributarias (OCDE, 2023).

5.4.41 Implementación internacional del CARF

El proceso de adopción global ha avanzado aceleradamente. Tras la publicación de los esquemas XML técnicos y las sucesivas actualizaciones del Foro

Global, un total de 76 jurisdicciones se encuentran formalmente comprometidas para materializar los primeros intercambios automáticos de información bajo el estándar CARF a partir de los ciclos previstos para 2027 y 2028 (OCDE, 2024; OCDE, 2025; OCDE, s. f.).

5.4.42 DAC8 en la Unión Europea

En sintonía con los estándares globales, la Unión Europea implementó la Directiva DAC8, con aplicación efectiva desde el 1 de enero de 2026, obligando a los prestadores de servicios a recopilar y reportar información transaccional de residentes europeos (Comisión Europea, s. f.). Conviene distinguir conceptualmente:

MiCa: Regulación de los mercados y emisión de criptoactivos.

DAC8: Cooperación administrativa y transparencia fiscal.

5.4.43 Impacto del nuevo sistema de transparencia sobre la fiscalización

La convergencia del CARF, el CRS modificado y la DAC8 reduce drásticamente la asimetría informativa histórica. Las administraciones tributarias transitan de un modelo limitado a cuentas bancarias tradicionales a un ecosistema de visibilidad total que integra pasarelas fiduciarias, intercambios descentralizados, transferencias y la identificación plena de los titulares (OCDE, 2023).

5.4.44 Fiscalidad internacional y auditoría forense

Desde la óptica forense, la información tributaria se contrasta mediante una secuencia analítica de validación cruzada:

declaración tributaria ingresosadquisicionesexchangewalletblockchainswapsdisposiciónbanco

El propósito central de la auditoría consiste en verificar la coherencia económica integral: que las rentas declaradas justifiquen las adquisiciones, que los costos posean respaldo documental idóneo y que las billeteras investigadas guarden correspondencia con el perfil patrimonial del contribuyente.

5.4.1 Conciliación contable-tributaria

Para entidades obligadas a llevar contabilidad formal, se recomienda implementar una matriz de conciliación para identificar diferencias temporarias y permanentes:

Concepto	Tratamiento Contable (NIIF)	Tratamiento Tributario
Saldo inicial	Registrado según política	Registrado según base fiscal
Adquisiciones	Costo de incorporación	Costo fiscal inicial
Revaluaciones	Reconocidas (si aplica modelo revaluación)	Puede diferirse hasta la realización
Deterioro	Reconocimiento en resultados	Sujeto a restricción legal de deducibilidad
Ganancias no realizadas	Conforme a NIIF aplicable	Conforme a la realización legal
Ventas / Disposición	Baja en libros según política	Cálculo de ganancia/pérdida realizada
Saldo final	Importe en libros al cierre	Costo fiscal remanente

5.4.2 Registro fiscal mínimo por operación

Para garantizar una defensa técnica sólida ante cualquier proceso de fiscalización o peritaje, el contribuyente debe conservar un registro operativo estructurado que contenga al menos los siguientes campos de trazabilidad:

Campo	Información requerida
Fecha, hora y zona horaria	Determinación precisa del período fiscal
Activo y Red	Denominación del criptoactivo y red blockchain
Cantidad y Tipo de operación	Unidades transadas y naturaleza (compra, venta, *swap*, *staking*)
Valor fiduciario y Fuente	Base de cálculo y proveedor o *exchange* de referencia
Tipo de cambio y Costo fiscal	Conversión aplicable y base patrimonial atribuible
Comisiones y Contraparte	Costos transaccionales y datos de identificación
Evidencia (TxID / Exchange)	Soporte técnico *on-chain* y comprobante *off-chain*
Resultado y Declaración fiscal	Ganancia/pérdida obtenida y formulario de reporte

5.4.1 Matriz tributaria integral de operaciones con criptoactivos

Operación	Potencial consecuencia en renta	IVA/GST	Riesgo internacional
Compra con fiat	Generalmente establece costo fiscal	Depende del régimen	Bajo/moderado
Venta por fiat	Posible ganancia/ pérdida	Exchange puede estar exento/fuera de alcance según jurisdicción	Alto si exchange extranjero
Cripto-cripto	Posible disposición fiscal	Generalmente tratamiento especial del medio de pago	Alto
Pago de bien	Posible disposición del criptoactivo	El bien puede continuar gravado	Moderado
Pago de servicio	Posible disposición	Servicio puede estar gravado	Moderado/alto
Minería	Renta al recibir o disponer, según jurisdicción	Tratamientos diversos	Moderado
Staking	Recompensa potencialmente imponible	Depende de actividad	Alto
Airdrop	Tratamiento variable	Variable	Moderado
Hard fork	Tratamiento variable	Variable	Moderado
NFT	Ganancia/renta según naturaleza	Puede existir IVA/ GST sobre la operación	Alto
DeFi	Depende de derechos transferidos	Alta complejidad	Muy alto
Transferencia entre wallets propias	Normalmente requiere demostrar que no hubo disposición	Normalmente sin suministro	Alto riesgo probatorio
Donación/herencia	Posible impuesto patrimonial/ sucesorio	Generalmente no equivalente a venta ordinaria	Moderado
Transferencia a wallet externa	Puede ser simplemente transferencia o disposición	Depende	Alto riesgo de atribución

Fuente: Esta matriz posee naturaleza analítica. No sustituye las disposiciones tributarias de cada jurisdicción.

5.4.2 Ejemplo integral de determinación fiscal

Supóngase que un contribuyente realiza las siguientes operaciones:

Compra 1 BTC por 20,000 u.m.

Posteriormente intercambia ese BTC por 10 ETH cuando el BTC vale 50,000 u.m.

Tiempo después utiliza 2 ETH para adquirir un bien valorado en 15,000 u.m.

Primera operación (Compra de BTC):

Costo fiscal inicial = 20,000 u.m.

En principio, la operación establece la base fiscal, sujeta a la legislación aplicable.

Segunda operación (Intercambio BTC → ETH):

Si la jurisdicción considera el intercambio cripto-cripto como realización:

Valor de disposición: 50,000 u.m.

Costo BTC: 20,000 u.m.

Ganancia potencial: 30,000 u.m.

Nuevo costo de los 10 ETH: 50,000 u.m., sujeto a las reglas locales (Costo unitario: 50,000/10=5,000 u.m.).

Tercera operación (Adquisición de bien con ETH):

Se utilizan 2 ETH para comprar un bien de 15,000 u.m.

Costo fiscal de los 2 ETH: 2×5,000=10,000 u.m.

Valor de disposición: 15,000 u.m.

Potencial ganancia: 15,000−10,000=5,000 u.m.

Adicionalmente, la adquisición del bien podrá encontrarse sometida al impuesto al consumo que corresponda.

Por consiguiente, en un régimen de realización de estas operaciones podrían existir dos hechos fiscales distintos, aunque solamente la primera operación involucró originalmente moneda fiduciaria.

Este ejemplo permite comprender por qué una revisión basada exclusivamente en **"**entradas y salidas bancarias**"** resulta insuficiente para determinar las obligaciones tributarias derivadas de criptoactivos.

5.4.3 Riesgos tributarios relevantes en auditoría forense

Entre las principales señales que justifican procedimientos adicionales pueden encontrarse:

- Elevado volumen de operaciones en exchanges sin reflejo tributario.
- Conversiones cripto-a-cripto omitidas.
- Costo fiscal sin documentos de adquisición.

- Transferencias hacia wallets no identificadas.
- Utilización de wallets personales por entidades.
- Diferencias entre declaración fiscal y extractos del exchange.
- Pérdidas declaradas sin evidencia de disposición.
- Supuestas pérdidas de claves sin documentación técnica.
- Ingresos de minería o staking no conciliados.
- Utilización inconsistente de precios.
- Cambios de metodología destinados a reducir ganancias.
- Transferencias transfronterizas sin identificación de contraparte.
- Fondos recibidos desde exchanges extranjeros sin explicación económica.
- Adquisición de criptoactivos incompatible con los ingresos declarados.

Estos elementos constituyen indicadores de riesgo, no evidencia automática de evasión tributaria, fraude o lavado de activos.

5.4.4 Relación entre evasión tributaria y lavado de activos

Debe evitarse equiparar ambos fenómenos. La evasión tributaria y el lavado de activos poseen elementos jurídicos diferentes y su configuración depende de las legislaciones penales y tributarias de cada jurisdicción.

No obstante, desde una perspectiva forense pueden utilizar estructuras operativas similares:

wallets múltiples → exchanges extranjeros → P2P → swaps → stablecoins → DeFi → autocustodia

La investigación debe determinar la finalidad y sustancia económica de las operaciones antes de formular conclusiones. El marco CARF fue desarrollado precisamente ante el riesgo de que operaciones internacionales con criptoactivos reduzcan la capacidad de las administraciones tributarias para verificar el correcto cumplimiento de las obligaciones fiscales (OCDE, 2023; OCDE, 2025).

5.4.5 Principio de trazabilidad fiscal

Para efectos del presente Manual puede proponerse el siguiente modelo secuencial:

Origen de fondos ↓ Adquisicion del criptoactivo ↓ ↓ Costo fiscal ↓ Wallet / Exchange ↓ Operaciones intermedias ↓ Disposicion ↓ Valor de realización ↓ Ganancia o pérdida ↓ Declaración tributaria ↓ Pago del impuesto

La reconstrucción debe poder efectuarse igualmente en sentido inverso. Esta trazabilidad permite verificar cuatro cuestiones fundamentales: existencia → titularidad/control → valoración → tributación.

5.4.6 Perspectiva futura de la fiscalidad internacional de criptoactivos

El principal cambio observable ya no se limita a definir cómo tributan los criptoactivos, sino que alcanza una segunda cuestión: ¿cómo conocerán las administraciones tributarias las operaciones realizadas fuera de sus fronteras?

El CRS resolvió parcialmente este problema respecto de cuentas financieras tradicionales. CARF busca extender la lógica de transparencia automática hacia determinados criptoactivos, mientras DAC8 desarrolla una respuesta regional en la Unión Europea. La OCDE ya dispone de esquemas XML específicamente diseñados para transmitir información CARF entre administraciones tributarias y actualizó técnicamente dichos formatos en 2025, evidenciando que el estándar se encuentra en una fase operativa de implementación (OCDE, 2025).

Por consiguiente, la evolución previsible es hacia una menor dependencia exclusiva de la declaración espontánea del contribuyente y una mayor utilización de información de terceros e intercambio internacional automatizado.

5.4.7 Criterio integrador sobre tributación y fiscalidad internacional

El tratamiento tributario de los criptoactivos debe construirse mediante un proceso secuencial:

- Identificación del activo.
- Determinación de los derechos económicos involucrados.
- Identificación del contribuyente.
- Determinación de su residencia fiscal.
- Caracterización de la operación.
- Identificación del hecho imponible.
- Determinación del momento de realización o reconocimiento.
- Determinación del costo fiscal.
- Valoración en moneda tributaria.
- Cálculo de la ganancia, pérdida o renta.
- Evaluación del impuesto al consumo u otros tributos.

- Determinación de la fuente de la renta.
- Aplicación del convenio internacional, cuando corresponda.
- Evaluación de obligaciones de información nacional e internacional.
- Conservación de evidencia documental y blockchain.

En consecuencia, la mera utilización de blockchain no crea ni elimina una obligación tributaria. Lo determinante continúa siendo la naturaleza jurídica y económica del hecho, la legislación fiscal aplicable y la vinculación tributaria del contribuyente con la jurisdicción correspondiente.

La evidencia internacional demuestra, además, que los sistemas tributarios mantienen diferencias sustanciales sobre la clasificación de las criptomonedas, el tratamiento de intercambios, minería, staking, airdrops y demás operaciones. Por ello resulta incorrecto extrapolar el tratamiento fiscal de un país hacia otro sin analizar previamente su normativa (OCDE, 2020; Baer et al., 2023).

Simultáneamente, la fiscalidad internacional está evolucionando hacia un modelo de mayor transparencia e intercambio automático de información. El CARF de la OCDE constituye el principal estándar global dirigido específicamente a operaciones con criptoactivos, mientras que la Unión Europea ha iniciado desde el 1 de enero de 2026 la aplicación del régimen DAC8 para ampliar el intercambio automático de información tributaria sobre estas operaciones (OCDE, 2023; Comisión Europea, s. f.).

Desde la perspectiva de la auditoría forense, este nuevo escenario permite integrar cuatro dimensiones que históricamente se encontraban fragmentadas:

Evidencia contable+Evidencia bancaria+Evidencia blockchain+Información tributaria internacional

La correcta correlación de estas fuentes puede permitir reconstruir no solamente la existencia y movimiento de los activos virtuales, sino también determinar su origen económico, costo fiscal, resultado obtenido, jurisdicción involucrada y eventual correspondencia con las declaraciones tributarias presentadas.

Por consiguiente, la fiscalidad de los criptoactivos debe entenderse actualmente no solo como un problema de determinación del impuesto, sino también como un problema de trazabilidad, información, cooperación internacional y capacidad probatoria.

5.5 Riesgos contables y financieros

La incorporación de criptoactivos en las operaciones de personas y entidades introduce una combinación de riesgos que excede los asociados tradicionalmente con activos financieros o intangibles. A los riesgos convencionales

de precio, liquidez, contraparte y crédito se agregan riesgos vinculados con la custodia de claves criptográficas, vulnerabilidades tecnológicas, funcionamiento de protocolos descentralizados, fragmentación de mercados, manipulación de precios, incertidumbre regulatoria, pérdida de acceso, fallas de *smart contracts* y dificultades para identificar la titularidad económica de determinados activos.

El *Financial Stability Board* (FSB) ha señalado que los diferentes segmentos del ecosistema criptoactivos sin respaldo, stablecoins y finanzas descentralizadas (DeFi) se encuentran estrechamente interrelacionados y deben evaluarse de manera integral. Asimismo, advierte que el crecimiento del sector y su creciente vinculación con el sistema financiero tradicional pueden incrementar los riesgos para la estabilidad financiera (FSB, 2025).

El Banco de Pagos Internacionales ha identificado, además, características estructurales particulares del ecosistema cripto, entre ellas congestión, altos costos de transacción, fragmentación, concentración de determinadas funciones pese a la apariencia de descentralización y amplificación en DeFi de riesgos ya conocidos en las finanzas tradicionales (BIS, 2023).

Desde el punto de vista del presente Manual, resulta útil distinguir inicialmente dos dimensiones:

- **Riesgos contables:** aquellos que pueden originar reconocimiento, medición, clasificación, presentación o revelación incorrectos en los estados financieros.
- **Riesgos financieros:** aquellos capaces de producir pérdidas económicas, restricciones de liquidez, deterioro patrimonial, incumplimiento de obligaciones o exposición significativa a variaciones adversas del mercado.

Ambas categorías se encuentran estrechamente vinculadas. Una caída significativa del precio constituye inicialmente un riesgo financiero; sin embargo, si la entidad no aplica correctamente el modelo de medición o deterioro correspondiente, también genera un riesgo de incorrección material contable.

5.5.1 Enfoque de riesgos aplicado a los criptoactivos

El análisis de riesgos no debe limitarse a establecer que una entidad "posee criptomonedas". Es necesario identificar la naturaleza concreta del activo, su utilización, modalidad de custodia, mercados utilizados, contrapartes, protocolos involucrados y relevancia cuantitativa y cualitativa para la entidad.

La NIA 315 (Revisada 2019) establece un proceso dirigido a identificar y valorar los riesgos de incorrección material mediante la comprensión de la en-

tidad, su entorno, el marco de información financiera aplicable y su sistema de control interno (IAASB, 2019).

En materia de criptoactivos, este análisis requiere comprender al menos:

- Naturaleza de las operaciones.
- Volumen y frecuencia.
- Finalidad de la tenencia.
- Wallets utilizadas.
- Exchanges y custodios.
- Personas con acceso.
- Procedimientos de autorización.
- Políticas contables.
- Fuentes de valoración.
- Redes blockchain.
- Protocolos DeFi.
- Mecanismos de conciliación.
- Exposición a cambios regulatorios.
- Controles sobre información tecnológica.

Por tanto, el riesgo debe analizarse desde la operación económica hasta su presentación final en los estados financieros.

5.5.2 Riesgo de clasificación contable incorrecta

Uno de los principales riesgos contables consiste en clasificar incorrectamente el criptoactivo. Como se desarrolló en el numeral 5.1, no todos los activos digitales poseen la misma naturaleza económica. Una criptomoneda comprendida dentro de la decisión del IFRS Interpretations Committee puede quedar bajo la NIC 38 o la NIC 2, mientras que un token que represente un derecho contractual podría requerir análisis bajo la NIC 32 y la NIIF 9.

Por ello pueden producirse errores como:

Criptomoneda descentralizada → registrada como efectivo.

Activo mantenido para comercialización ordinaria → registrado como intangible.

Security token → registrado automáticamente como intangible.

Stablecoin → registrado automáticamente como efectivo.

Activo tokenizado → registrado como intangible ignorando el derecho subyacente.

La clasificación incorrecta afecta posteriormente la medición, reconocimiento de resultados, deterioro, presentación y revelaciones. Por tanto, un error inicial de clasificación puede propagarse a todo el tratamiento contable

posterior**.** Este riesgo debe considerarse particularmente relevante cuando la entidad utiliza la palabra genérica "criptoactivos" para agrupar instrumentos económicamente diferentes.

5.5.3 Riesgo de reconocimiento de activos inexistentes o no controlados

La existencia de un saldo asociado a una dirección blockchain no demuestra automáticamente que dicho saldo corresponda económicamente a la entidad. Pueden presentarse situaciones en las cuales:

La wallet pertenece a un tercero.

El activo se mantiene únicamente en custodia.

La entidad perdió definitivamente las claves.

La cuenta del exchange está bloqueada.

Existen derechos de terceros sobre los activos.

La dirección fue identificada incorrectamente.

Una captura de pantalla fue alterada.

Los activos se encontraban comprometidos contractualmente.

Consecuentemente, debe diferenciarse entre:

Existencia tecnológica → Acceso → Control → Titularidad económica → Reconocimiento contable

La comprobación de uno de estos elementos no acredita necesariamente los restantes. Desde una perspectiva de auditoría, la NIA 315 exige identificar riesgos de incorrección material en las afirmaciones relevantes, mientras que la obtención de evidencia suficiente y adecuada constituye el fundamento de la conclusión del auditor (IAASB, 2019).

5.5.4 Riesgo de omisión de criptoactivos

El problema inverso consiste en que existan activos controlados por la entidad que no aparezcan registrados en la contabilidad. Este riesgo resulta particularmente elevado cuando se utilizan:

- Wallets de autocustodia.
- Wallets creadas por empleados.
- Cuentas personales utilizadas para operaciones corporativas.
- Múltiples exchanges.
- Plataformas extranjeras.
- Protocolos DeFi.

- Wallets frías.
- Direcciones no incorporadas al sistema financiero interno.

Una entidad puede poseer simultáneamente decenas o cientos de direcciones. Por tanto, verificar únicamente las wallets declaradas por la administración puede no proporcionar evidencia suficiente acerca de la integridad del universo de activos. Desde una perspectiva forense, la investigación de integridad puede requerir analizar transferencias bancarias hacia exchanges, direcciones vinculadas, retiros, depósitos, documentación KYC, movimientos históricos y relaciones entre wallets.

5.5.5 5.5.5 Riesgo de doble contabilización

La utilización simultánea de blockchain, exchanges y sistemas contables puede originar duplicación de activos. Por ejemplo:

1 BTC permanece registrado en el auxiliar del exchange.

Posteriormente se efectúa el movimiento: Exchange → Wallet corporativa.

Si el sistema registra el retiro como una salida pero la wallet como una nueva adquisición, la contabilidad puede terminar reconociendo 2 BTC cuando económicamente existe únicamente 1 BTC.

Este fenómeno es especialmente frecuente cuando los sistemas importan separadamente archivos CSV del exchange, información de exploradores blockchain, extractos bancarios y registros manuales. Por ello, las transferencias internas deben identificarse antes de efectuar la contabilización definitiva.

5.5.6 Riesgo de valoración

La volatilidad y fragmentación de los mercados de criptoactivos convierten la valoración en una de las áreas de mayor riesgo de incorrección. Puede existir incertidumbre respecto de:

- Mercado principal.
- Exchange utilizado.
- Hora de corte.
- Zona horaria.
- Liquidez.
- Precio representativo.
- Existencia de mercado activo.
- Nivel de jerarquía del valor razonable.
- Conversión a moneda funcional.

- Tratamiento de costos de transacción.

La NIIF 13 establece que, cuando corresponde utilizar valor razonable, la medición debe representar el precio que se recibiría por vender el activo en una transacción ordenada entre participantes del mercado en la fecha de medición (IFRS Foundation, 2024). El riesgo aumenta cuando la administración puede escoger entre numerosos exchanges y seleccionar aquel que presente el precio que produzca el resultado financiero más favorable.

5.5.7 Riesgo de selección oportunista de precios

La disponibilidad simultánea de diferentes cotizaciones genera un riesgo específico de *price shopping* o selección oportunista de precios. Supóngase que un criptoactivo cotiza al cierre de la siguiente manera:

Mercado	Precio
Exchange A	98
Exchange B	103
Exchange C	95

No sería razonable que la entidad utilice sistemáticamente 103 para valorar activos y 95 para valorar pasivos o posiciones desfavorables sin que exista una justificación consistente con las NIIF. Por ello, la política de valoración debería definir antes del cierre:

Mercado → Fuente → Hora → Metodologı´a → Fuentes alternativas

El control preventivo es más confiable que seleccionar retrospectivamente el precio después de conocer el efecto sobre los estados financieros.

5.5.8 Riesgo por ausencia o pérdida de un mercado activo

Un activo puede haber tenido una cotización observable durante un período y posteriormente perder significativamente su liquidez. Esta situación es especialmente relevante para:

- Tokens de proyectos pequeños.
- NFTs.
- Tokens recientemente emitidos.
- Activos abandonados.
- Mercados suspendidos.

- Activos deslistados de exchanges.

Una última operación realizada semanas o meses antes puede no representar razonablemente las condiciones existentes en la fecha de medición. La NIIF 13 utiliza una jerarquía que otorga mayor prioridad a datos observables y menor prioridad a datos no observables; por tanto, a medida que disminuye la actividad de mercado, aumenta normalmente el juicio profesional requerido para efectuar la medición (Nivel 3).

5.5.9 Riesgo de deterioro

Los criptoactivos contabilizados como activos intangibles pueden encontrarse sujetos a la NIC 36, según corresponda. La volatilidad puede generar reducciones significativas de valor; sin embargo, el riesgo contable consiste tanto en no reconocer un deterioro que corresponde, como en reconocer pérdidas simplemente por variaciones temporales sin efectuar el análisis exigido por la norma.

Por ello debe distinguirse entre un precio inferior al costo y la existencia real de deterioro conforme a la NIC 36. Asimismo, cuando un activo intangible posea vida útil indefinida, la norma exige pruebas periódicas específicas. El riesgo aumenta cuando existen activos con poca liquidez, sin actividad reciente, asociados a proyectos abandonados o vinculados a protocolos vulnerados.

5.5.10 Riesgo de reconocimiento inadecuado de ganancias

La elevada volatilidad puede incentivar el reconocimiento anticipado de ganancias no realizadas. Por ejemplo:

- Costo: 100
- Precio observable al cierre: 180

El incremento de 80 no constituye automáticamente una ganancia reconocible en resultados. El tratamiento dependerá de la clasificación, la norma aplicable, el modelo de medición, la existencia de mercado activo y la naturaleza de la entidad. Confundir incremento de precio con ganancia contable realizada puede producir una sobrestimación significativa de resultados y patrimonio.

5.5.1 Riesgo de corte contable (*Cut-off*)

Los mercados de criptoactivos operan de manera continua (24/7). En consecuencia, pueden coexistir:

- Fecha de orden.
- Fecha de ejecución.
- Fecha registrada por el exchange.
- Timestamp blockchain.
- Confirmación y disponibilidad efectiva.
- Fecha local de la entidad.

Una operación registrada a las 00:30 UTC del 1 de enero puede corresponder todavía al 31 de diciembre en otra zona horaria. Por tanto, deben existir políticas específicas de *cut-off*. La ausencia de criterios uniformes puede trasladar activos, ganancias o pérdidas entre ejercicios diferentes.

5.5.2 Riesgo de registros contables incompletos

El registro puede ser incompleto cuando solamente se contabilizan las operaciones relacionadas con cuentas bancarias. Una entidad podría efectuar la cadena:

BTC → ETH → USDC → Token → BTC

sin que se produzca ninguna nueva transferencia bancaria. No obstante, cada intercambio posee consecuencias contables y potenciales efectos tributarios.

Por ello, la ausencia de movimiento bancario no significa ausencia de operación económica, constituyendo una diferencia fundamental entre la auditoría tradicional de tesorería y la investigación de activos virtuales.

5.5.3 Riesgo de presentación y revelación insuficiente

Los riesgos no terminan con el reconocimiento y medición. Una entidad puede contabilizar correctamente los activos pero proporcionar información insuficiente sobre las incertidumbres relevantes. La NIC 1 exige revelar fuentes significativas de incertidumbre en las estimaciones (párrs. 125-131) y la NIIF 7 exige información para evaluar la naturaleza y extensión de los riesgos derivados de instrumentos financieros (IFRS Foundation, 2024).

Pueden resultar relevantes según las circunstancias:

- Política de clasificación y valoración.
- Fuentes de precios y existencia de mercado activo.
- Juicios significativos y exposición material.
- Concentración y eventos posteriores.
- Restricciones de custodia e incertidumbres regulatorias.

5.5.4 Riesgo de mercado y volatilidad

Desde la perspectiva financiera, el riesgo de mercado constituye probablemente la exposición más evidente. La NIIF 7 define el riesgo de mercado como el riesgo de que el valor razonable o los flujos de efectivo futuros fluctúen como consecuencia de cambios en los precios de mercado (IFRS Foundation, 2024).

La volatilidad puede generar pérdidas rápidas, deterioro patrimonial, llamadas de margen, liquidaciones forzosas, incumplimiento de *covenants* y pérdidas de capacidad operativa. El FSB continúa señalando la elevada volatilidad como una vulnerabilidad relevante para la estabilidad financiera (FSB, 2026).

5.5.5 Riesgo de liquidez

Debe diferenciarse cuidadosamente el precio observable de la capacidad efectiva de liquidación. Una entidad puede observar que un token cotiza a 100 u.m., pero si posee una posición de gran tamaño en un mercado poco profundo, la venta completa podría provocar una caída drástica del precio. Por ello:

Valor de cotización =Efectivo necesariamente realizable por toda la posición

La liquidez puede deteriorarse rápidamente debido a la retirada de creadores de mercado, suspensión de retiros, cierre de exchanges, restricciones regulatorias, pérdida de confianza, congestión de red o desanclaje de una stablecoin (BIS, 2023).

5.5.6 Riesgo de concentración

La concentración puede adoptar diferentes formas dentro de la estructura patrimonial:

- **Por activo:** Proporción significativa en un solo criptoactivo.
- **Por exchange:** Mayoría de activos en una única plataforma.
- **Por custodio:** Una sola entidad controla las claves.
- **Por blockchain:** Actividad dependiente de una sola red.

- **Por stablecoin:** Liquidez vinculada a un único emisor.
- **Por protocolo:** Gran parte comprometida en una aplicación DeFi.

Una entidad aparentemente diversificada puede poseer un riesgo común elevado si todos los activos dependen de la misma blockchain, el mismo *bridge*, la misma stablecoin o el mismo custodio.

5.5.7 Riesgo de contraparte

Cuando los activos se mantienen mediante un tercero (exchange, custodio, broker, emisor, prestatario, contraparte OTC o proveedor DeFi), aparece el riesgo de incumplimiento. La quiebra o suspensión de un intermediario puede impedir recuperar los activos.

Desde una perspectiva contable, debe determinarse si la entidad continúa controlando directamente el criptoactivo o si posee un derecho creditorio frente al intermediario:

Activo depositado en terceroNecesariamente mismo derecho económico que activo bajo autocustodia

IOSCO ha identificado los riesgos de los proveedores centralizados como un área central de protección al inversionista y conflictos de interés (IOSCO, 2023).

5.5.8 Riesgo de custodia

La custodia constituye una de las particularidades más significativas de los criptoactivos, dividiéndose principalmente en **custodia propia** (la entidad controla las claves) y custodia de terceros (un proveedor gestiona el acceso). Cada modalidad genera riesgos distintos:

Riesgos en Autocustodia:

- Pérdida de claves y destrucción de dispositivos.
- Exposición de la *seed phrase*.
- Acceso no autorizado y falta de segregación de funciones.
- Inexistencia de procedimientos sucesorios y concentración del control.

Riesgos en Custodia de Terceros:

- Insolvencia y fraude del proveedor.
- Ataques informáticos (*hackeos*).
- Congelación o restricciones de retiro.
- Incertidumbre sobre segregación legal de activos.

Por tanto, eliminar el riesgo del custodio puede incrementar el riesgo de gestión de claves, mientras que delegar la custodia reduce el segundo pero introduce riesgo de contraparte.

Si deseas que revisemos, corrijamos o integremos alguna otra sección específica de tu manual, indícamelo con confianzas.

5.5.9 Riesgo de pérdida de claves privadas

Una característica distintiva de las redes blockchain es que la pérdida irreversible de las credenciales necesarias para realizar una transacción puede impedir permanentemente la disposición de los activos.

El problema contable consiste en determinar si la entidad continúa controlando un recurso económico del cual pueda obtener beneficios.

Desde la perspectiva forense debe distinguirse:

"No recuerdo la contraseña"

"La clave privada ha sido destruida irreversiblemente"

La segunda conclusión requiere evidencia técnica considerablemente más sólida. La simple declaración de una persona no debería considerarse, por sí misma, evidencia suficiente para justificar la desaparición contable de un activo material.

5.5.10 Riesgo de ciberseguridad

Los criptoactivos dependen directamente de infraestructura tecnológica. Entre las amenazas pueden encontrarse:

- Malware
- Phishing
- Robo de credenciales
- SIM swapping
- Vulnerabilidades de dispositivos
- Ataques a exchanges
- Compromisos de API
- Suplantación
- Ataques a interfaces web
- Manipulación de firmas

El riesgo tecnológico no se limita a *"hackear una blockchain"*. En muchos casos, el punto vulnerable es el usuario, dispositivo, custodio o aplicación periférica.

El FSB continúa situando la resiliencia operacional entre los aspectos relevantes para la estabilidad financiera, mientras que trabajos recientes del BIS destacan que los riesgos cibernéticos pueden afectar incluso mecanismos centrales de determinadas infraestructuras blockchain (FSB, 2026; BIS, 2026).

5.5.11 Riesgo de *smart contracts*

Los *smart contracts* permiten ejecutar automáticamente determinadas instrucciones cuando se cumplen condiciones programadas. Sin embargo, *"automático"* no significa *"libre de riesgo"*.

Pueden existir:

- Errores de programación
- Vulnerabilidades
- Lógica económica defectuosa
- Permisos administrativos ocultos
- Mecanismos de actualización
- Dependencia de terceros
- Fallas de gobernanza

Una entidad puede considerar que sus activos se encuentran *"depositados"* en un protocolo cuando jurídicamente y tecnológicamente ha transferido activos hacia un contrato cuyo funcionamiento depende de código que contiene riesgos específicos.

IOSCO ha señalado que DeFi reproduce múltiples actividades financieras tradicionales y plantea riesgos relacionados con conflictos, gobernanza, operación, asimetría de información e integridad de mercado (IOSCO, 2023).

5.5.12 Riesgo de oráculos

Muchos protocolos descentralizados requieren información externa a la blockchain —por ejemplo, precio ETH/USD, tipo de cambio o precio de un activo financiero— para ejecutar liquidaciones o calcular garantías. Esta información es suministrada por oráculos.

- Una falla o manipulación del oráculo puede ocasionar:
- Valoración incorrecta
- Liquidaciones indebidas
- Pagos incorrectos
- Pérdida de garantías
- Explotación del protocolo

Desde la perspectiva contable, la entidad debe comprender que el valor o rendimiento de determinados tokens puede depender de infraestructuras adicionales que no son evidentes mediante la simple observación de la wallet.

5.5.13 Riesgo de *bridges* y activos *wrapped*

Los *bridges* permiten trasladar valor entre diferentes blockchains; sin embargo, normalmente introducen una infraestructura adicional que puede convertirse en un punto de vulnerabilidad.

Por ejemplo:

- BTCbridgeWrapped BTC en otra red
- El activo resultante puede depender de:
- Custodio
- Contrato inteligente
- Mecanismo de bloqueo
- Validadores
- Reservas subyacentes

El BIS ha destacado que los mecanismos utilizados para superar la fragmentación entre cadenas, como los *bridges*, introducen sus propios riesgos (BIS, 2026). Por tanto, no debe asumirse que:

1wrapped token} = 1activo original

sin analizar la estructura que sustenta dicha equivalencia.

5.5.14 Riesgo de *stablecoins* y pérdida de paridad

La denominación *stablecoin* puede generar una percepción incorrecta de ausencia de riesgo. En realidad, pueden existir:

Riesgo del emisor
Riesgo de reservas
Riesgo bancario
Riesgo de liquidez
Riesgo tecnológico
Riesgo de reembolso
Riesgo regulatorio
Riesgo de desanclaje

El FSB ha identificado específicamente el riesgo de corrida en *stablecoins* y mantiene durante 2026 el seguimiento de su creciente vinculación con el sistema financiero tradicional (FSB, 2025).

Ahmed, Aldasoro y Duley (2024/2025) muestran que la estabilidad de la paridad depende, entre otros factores, de la calidad y volatilidad percibida de las reservas y de las condiciones de conversión. Cuando los activos de respaldo son altamente volátiles, *shocks* negativos suficientemente grandes pueden comprometer la paridad incluso con niveles inicialmente elevados de respaldo.

De igual manera, Aldasoro et al. (2024) observan que estructuras en las cuales pasivos semejantes al dinero se respaldan con activos potencialmente menos líquidos pueden generar riesgos de corrida similares, en algunos aspectos, a los existentes en fondos de mercado monetario. Por ello: stablecoin no significa activo libre de riesgo.

5.5.15 Riesgo de crédito

Cuando un criptoactivo representa un derecho contractual frente a una contraparte, puede existir auténtico riesgo de crédito. La NIIF 7 define el riesgo de crédito como el riesgo de que una parte de un instrumento financiero cause una pérdida financiera a otra al incumplir una obligación (IFRS Foundation, 2024).

Este riesgo puede resultar relevante para:

- Tokens de deuda
- Préstamos DeFi
- *Stablecoins* con derecho contractual
- Activos tokenizados
- Depósitos con custodios
- Créditos otorgados mediante plataformas

Cuando el instrumento se encuentra bajo NIIF 9 también puede resultar aplicable el modelo de pérdidas crediticias esperadas, dependiendo de su clasificación. Por tanto, la tecnología blockchain no elimina el riesgo de incumplimiento del obligado.

5.5.16 Riesgo de apalancamiento y liquidaciones automáticas

Las plataformas centralizadas y los protocolos DeFi pueden permitir obtener exposición mediante préstamos, derivados, futuros, margen y posiciones apalancadas. El apalancamiento amplifica tanto ganancias como pérdidas.

Por ejemplo:

- Patrimonio: 100

- Exposición económica: 500

Una disminución relativamente pequeña del precio puede consumir una proporción considerable del patrimonio. En DeFi, además, determinadas liquidaciones pueden ejecutarse automáticamente mediante *smart contracts*, lo que reduce la posibilidad de negociar una extensión o refinanciamiento una vez alcanzados determinados parámetros.

En períodos de estrés pueden producirse dinámicas de:

caída de precioliquidacionesventas adicionalesnueva caída de precionuevas liquidaciones

El BIS ha señalado que DeFi puede amplificar riesgos conocidos de las finanzas tradicionales y que la interconexión interna del ecosistema puede intensificar episodios de tensión (BIS, 2023).

5.5.17 Riesgo de liquidez en protocolos DeFi

El valor indicado por un protocolo puede no coincidir con el importe que podría obtenerse al retirar o intercambiar una posición significativa. Pueden existir:

- *Slippage*
- Falta de profundidad
- Períodos de bloqueo
- Mecanismos de gobernanza
- Congestión
- Reducción de liquidez
- Pérdida impermanente
- Riesgos asociados al *pool*

Por ello debe distinguirse el **valor teórico de la posición** del **importe efectivamente realizable**. Este análisis resulta indispensable cuando las posiciones son materiales respecto del patrimonio de la entidad.

5.5.18 Riesgo de manipulación de mercado

Los mercados de criptoactivos pueden presentar estructuras distintas de los mercados financieros regulados tradicionales. Entre las conductas potencialmente relevantes pueden encontrarse:

- *Wash trading*
- Operaciones coordinadas
- *Pump and dump*

- Manipulación de libros de órdenes
- Información privilegiada
- Volúmenes artificiales
- Operaciones entre partes relacionadas

La IOSCO desarrolló sus recomendaciones globales para mercados de criptoactivos alrededor de áreas como integridad de mercado, conflictos de interés, abuso de mercado, custodia y protección de activos de clientes (IOSCO, 2023). Desde la perspectiva contable, una cotización generada en un mercado manipulado puede afectar directamente la fiabilidad de una valoración.

5.5.19 Riesgo de fraude

Los criptoactivos pueden ser utilizados dentro de esquemas fraudulentos, aunque su utilización no constituye por sí misma prueba de fraude. Entre los riesgos pueden encontrarse:

- Activos inexistentes
- Wallets falsamente atribuidas
- Balances manipulados
- Comprobantes falsos de *exchange*
- Esquemas Ponzi
- *Rug pulls*
- Apropiación de claves
- Operaciones con partes relacionadas no reveladas
- Valoración artificial
- Ocultamiento de pérdidas
- Creación de tokens sin sustancia económica

La NIA 240 revisada fortalece expresamente el enfoque de fraude dentro de la identificación y valoración de riesgos y exige respuestas más robustas frente a los riesgos identificados (IAASB, 2025). En una investigación forense debe mantenerse una distinción metodológica fundamental: indicador de fraude prueba de fraude**.** La conclusión requiere corroboración mediante evidencia suficiente, pertinente y confiable.

5.5.20 Riesgo de lavado de activos y financiamiento ilícito

La transferibilidad global, pseudonimidad, operaciones P2P y capacidad de desplazar activos entre múltiples plataformas pueden generar riesgos relevan-

tes de lavado de activos y financiamiento ilícito. El GAFI ha desarrollado un marco específico para activos virtuales y proveedores de servicios de activos virtuales (Grupo de Acción Financiera Interamericana [GAFI], 2025).

Entre los factores que pueden requerir análisis adicional se encuentran:

- Transferencias sin justificación económica
- Utilización intensiva de múltiples wallets
- Exposición a servicios de alto riesgo
- Operaciones con jurisdicciones sin regulación adecuada
- Transferencias P2P incompatibles con el perfil económico
- Utilización de activos destinados a ocultar la trazabilidad
- Discrepancias entre KYC, contabilidad y beneficiario económico

Sin embargo, ninguna de estas circunstancias permite concluir automáticamente la existencia de lavado de activos.

5.5.21 Riesgo regulatorio y jurídico

El marco jurídico de los criptoactivos continúa evolucionando y presenta diferencias significativas entre jurisdicciones. Un mismo activo puede encontrarse autorizado en un país, restringido en otro, sometido a regulación de valores en un tercero, sujeto a requisitos específicos de licencia o prohibido para determinados intermediarios.

El FSB señaló en su revisión temática de 2025 que persisten brechas e inconsistencias significativas en la implementación de los marcos regulatorios aplicables, lo que puede favorecer arbitraje regulatorio y dificultar la supervisión transfronteriza (FSB, 2025). Por consiguiente, el riesgo regulatorio puede afectar:

- Disponibilidad de mercados
- Capacidad de retiro
- Valoración
- Continuidad del negocio
- Obligaciones de reporte
- Custodia
- Tributación

5.5.22 Riesgo tributario

Los riesgos tributarios se encuentran estrechamente relacionados con el apartado 5.4. Pueden surgir por:

- Omisión de operaciones cripto-cripto
- Determinación incorrecta del costo fiscal
- Falta de documentación
- Clasificación errónea
- Aplicación incorrecta del tipo de cambio
- Falta de declaración de recompensas
- Operaciones transfronterizas
- Obligaciones de información

Con la progresiva implementación del CARF y sistemas regionales como DAC8, la conciliación entre contabilidad + blockchain + exchange + declaración tributaria debe formar parte del sistema de control.

5.5.23 Riesgo de tipo de cambio

Aunque determinadas criptomonedas no constituyen monedas para efectos de las NIIF, las operaciones pueden cotizarse en monedas diferentes de la moneda funcional de la entidad (por ejemplo, BTC/USD para una entidad cuya moneda funcional es PEN).

La valoración requiere combinar:

Cantidad BTCPrecio BTC/USDTipo de cambio USD/PEN

Una incorrección en cualquiera de los tres componentes afecta el resultado. Asimismo, debe evitarse utilizar cotizaciones correspondientes a horas distintas cuando la volatilidad sea material.

5.5.24 Riesgo operativo

El riesgo operativo comprende fallas de personas, procedimientos, sistemas o proveedores externos. Puede materializarse mediante:

- Envío a dirección incorrecta
- Selección de blockchain incorrecta
- Pérdida de dispositivos
- Aprobación insuficiente
- Error en cantidad
- Configuración defectuosa de wallets
- Conciliaciones incompletas
- Fallas de API
- Errores en software contable
- Errores de conversión

Una característica especialmente relevante es la irreversibilidad práctica de muchas transferencias blockchain, ya que a diferencia de la banca tradicional, una transferencia correctamente confirmada hacia una dirección equivocada suele carecer de un mecanismo central de reversión.

5.5.25 Riesgo de segregación de funciones

La concentración de facultades en una sola persona constituye un riesgo crítico. Una persona que pueda simultáneamente crear una wallet, custodiar la clave, iniciar una transferencia, aprobarla y registrarla contablemente posee capacidad para ejecutar y ocultar una operación.

Un control más robusto debería separar, cuando la estructura de la entidad lo permita:

CustodiaAutorizaciónEjecuciónRegistroConciliación

Las wallets multifirma (*multisignature*) contribuyen técnicamente a implementar controles de aprobación múltiple, aunque no sustituyen los restantes controles administrativos.

5.5.26 Riesgo de personas clave

Una entidad puede depender excesivamente de una sola persona que conoce claves, *seed phrases*, procedimientos de recuperación, cuentas de exchanges y ubicación de dispositivos. La enfermedad, fallecimiento, separación laboral o conflicto con dicha persona puede ocasionar pérdida de acceso.

Por tanto, el riesgo de persona clave debe incorporarse al diseño de continuidad operativa, buscando un equilibrio entre redundancia suficiente para asegurar continuidad y restricción suficiente para impedir accesos no autorizados.

5.5.27 Riesgo relacionado con terceros proveedores

El ecosistema puede depender de exchanges, custodios, proveedores de precios, APIs, exploradores blockchain, servicios de analítica, proveedores de infraestructura y proveedores de nodos. La interrupción o alteración de uno de estos servicios puede afectar la ejecución, valoración, conciliación, información financiera y evidencia disponible.

5.5.28 Riesgo de dependencia de información proporcionada por *exchanges*

Un estado de cuenta descargado desde un exchange constituye evidencia relevante, pero no necesariamente suficiente por sí sola, ya que el exchange puede mantener registros internos, agrupar fondos, utilizar direcciones colectivas o ejecutar operaciones fuera de cadena.

La información debe conciliarse con extractos bancarios, archivos del exchange, la blockchain y los registros contables. La NIA 500 enfatiza la necesidad de evaluar la fiabilidad de la información utilizada como evidencia (IAASB, 2026).

5.5.29 Riesgo de evidencia digital insuficiente

Entre los errores frecuentes de auditoría o peritaje pueden encontrarse:
Utilizar únicamente capturas de pantalla
No registrar fecha y hora
Omitir la dirección completa
No conservar el TxID
No identificar la blockchain
Confiar en información preparada exclusivamente por la parte examinada
No verificar la propiedad económica

Por ejemplo, una captura de pantalla con el texto *"Saldo 10 BTC"* no demuestra por sí misma que el saldo exista, que pertenezca al examinado, que corresponda a la fecha investigada, que no haya sido alterada o que el usuario pudiera disponer de los activos.

5.5.30 Riesgo de información histórica incompleta

Con el paso del tiempo pueden desaparecer exchanges, historiales, cuentas de correo, dispositivos, claves o plataformas. Una blockchain pública puede conservar la transacción, pero no necesariamente la identidad de sus participantes. Por ello, la conservación documental debe contemplar tanto la información *on-chain* como *off-chain*.

5.5.1 Riesgo de correlación entre criptoactivos

La diversificación aparente puede no reducir significativamente el riesgo cuando los activos presentan una elevada correlación durante períodos de estrés.

Portafolio	Participación
BTC	30 %
ETH	25 %
Token A	15 %
Token B	15 %
Token C	15 %

A simple vista existen cinco activos, pero ante condiciones adversas todos podrían sufrir movimientos simultáneos. Debe evaluarse la correlación, la liquidez y los factores comunes subyacentes.

5.5.2 Riesgo de interconexión y contagio

El ecosistema cripto presenta múltiples conexiones internas (por ejemplo: stablecoinexchangeprotocolo DeFitoken colateral). Una falla en uno de estos componentes puede propagarse hacia los restantes, por lo que una evaluación centrada en un solo activo subestima las dependencias reales (FSB, 2025).

5.5.3 Riesgo sistémico

La acumulación de exposiciones puede alcanzar una dimensión sistémica capaz de amenazar la estabilidad financiera (FSB, 2026). A nivel empresarial, este riesgo se manifiesta mediante crisis general de liquidez, pérdida de acceso bancario, desanclaje de *stablecoins* o cierre simultáneo de plataformas.

5.5.1 Riesgo de negocio en entidades altamente expuestas

Una entidad puede depender materialmente de la evolución de los criptoactivos para sus ingresos, pagos, financiación, garantías, liquidez o reservas, incluso si estos representan solo una parte de su balance. Una contracción del ecosistema afectaría su modelo de negocio completo.

5.5.2 Riesgo de negocio en marcha

Cuando las pérdidas asociadas con activos virtuales afectan materialmente la liquidez o solvencia, puede evaluarse el principio de negocio en marcha ante señales como pérdida material de activos, insolvencia del custodio, caída extrema de precios o bloqueo de retiros (IAASB, 2025).

Tabla No. 5 Matriz integrada de riesgos

Riesgo	Posible efecto	Evidencia / procedimiento relevante
Clasificación	Aplicación de NIIF incorrecta	Revisar derechos y finalidad
Existencia	Activos ficticios	Blockchain + confirmación
Integridad	Activos omitidos	Bancos + exchanges + wallets
Control	Registro de activos de terceros	Contratos + claves / custodia
Valuación	Activos sobre / subvaluados	Mercado, precio y metodología
Corte	Período incorrecto	Timestamp + zona horaria
Deterioro	Resultados incorrectos	NIC 36 + evidencia de mercado
Liquidez	Incapacidad de realizar activos	Volumen y profundidad
Mercado	Pérdidas por volatilidad	Sensibilidad y exposición
Contraparte	Pérdida por incumplimiento	Solvencia y condiciones contractuales
Custodia	Pérdida / acceso restringido	Política de claves / custodio
Stablecoin	Pérdida de paridad	Reservas y reembolso
Smart contract	Pérdida tecnológica	Auditorías del protocolo
Bridge	Pérdida / interrupción	Estructura de respaldo
Ciberseguridad	Sustracción de activos	Logs y controles
Fraude	Apropiación / manipulación	Procedimientos forenses
AML/CFT	Riesgo legal / reputacional	KYC y trazabilidad

Tributario	Contingencias fiscales	Conciliación fiscal
Regulatorio	Restricción / prohibición	Monitoreo normativo
Concentración	Pérdida material	Exposición por activo / proveedor
Terceros	Interrupción / pérdida	Due diligence de proveedores

Tabla No. 6

Matriz de riesgos por afirmación contable

Afirmación	Riesgo en criptoactivos	Procedimiento principal
Existencia	Saldo ficticio	Verificación blockchain / exchange
Derechos y obligaciones	Wallet de terceros	Titularidad y contratos
Integridad	Wallets ocultas	Rastrear fondos y contrapartes
Valuación	Precio inadecuado	NIIF 13 / fuente independiente
Exactitud	Unidades o costos incorrectos	Recalcular
Corte	Timestamp en período incorrecto	UTC / zona horaria
Clasificación	NIC 38 vs. NIC 2 vs. NIIF 9	Analizar sustancia
Presentación	Agrupación inadecuada	Revisar estados financieros
Revelación	Riesgos materiales omitidos	Revisar notas y juicios

5.5.3 Indicadores de riesgo o *red flags*

En auditoría forense, determinadas circunstancias justifican procedimientos adicionales:

- Wallets no reveladas
- Uso de cuentas personales para activos empresariales
- Diferencias inexplicadas entre blockchain y contabilidad
- Operaciones con precios alejados del mercado
- Transferencias hacia partes relacionadas
- Múltiples movimientos sin sustancia económica aparente
- Grandes transferencias inmediatamente antes del cierre
- Utilización de exchanges sin KYC
- Pérdidas recurrentes sin documentación
- Modificación retrospectiva de costos
- Tokens de baja liquidez utilizados para justificar patrimonio elevado

- Transferencias internas registradas como ventas
- Compras sin fuente de fondos identificable
- Activos supuestamente perdidos sin evidencia técnica
- Saldos significativos sustentados únicamente mediante capturas de pantalla

Ninguno de estos indicadores constituye prueba concluyente; su función es orientar la extensión y naturaleza de los procedimientos de investigación.

5.5.4 Evaluación de probabilidad e impacto

Para efectos prácticos, los riesgos se evalúan combinando la probabilidad de ocurrencia y el impacto potencial:

Probabilidad / Impacto	Bajo	Medio	Alto
Baja	Bajo	Bajo / medio	Medio
Media	Bajo / medio	Medio	Alto
Alta	Medio	Alto	Crítico

Ejemplo 1: Pérdida de la clave privada de una wallet con el 1 % del patrimonio Impacto moderado.

Ejemplo 2: Pérdida de la clave privada de una wallet con el 70 % de los activos líquidos Impacto crítico.

Por tanto, el riesgo depende tanto de la vulnerabilidad tecnológica como de la materialidad económica de la exposicións.

5.5.5 Controles internos mínimos

Una entidad con exposición material a activos virtuales debería implementar, en función de su tamaño y complejidad:

- Inventario formal de wallets y cuentas.
- Segregación entre wallets personales y corporativas.
- Procedimientos de aprobación.
- Segregación de funciones.
- Multifirma cuando resulte apropiado.
- Custodia segura de claves y mecanismos de recuperación.
- Registro auxiliar de unidades y costos.
- Conciliación periódica blockchain–exchange–contabilidad.
- Política de valoración.

- Lista de exchanges y custodios autorizados.
- Control sobre partes relacionadas.
- Monitoreo tributario y regulatorio.
- Respaldo de evidencia digital.
- Plan de respuesta frente a incidentes.
- Procedimientos de continuidad operativa.

El objetivo no es eliminar completamente el riesgo lo cual resulta imposible, sino reducirlo a niveles compatibles con la tolerancia al riesgo y la materialidad de la entidad.

5.5.6 Riesgo de interpretar incorrectamente la blockchain

Una blockchain ofrece información altamente útil, pero no responde automáticamente todas las preguntas contables o forenses.

Puede demostrar:

- qué dirección enviócuántoa qué direccióncuándo
- No necesariamente demuestra:
- Quién controla la dirección.
- Por qué se realizó.
- Qué contrato existe.
- cuál es su tratamiento contable.
- Si la operación es lícita.
- Por ello debe evitarse una conclusión como:
- *"La blockchain demuestra que la persona X transfirió los fondos."*
- cuando la evidencia únicamente demuestra que:
- *"la dirección A transfirió los fondos hacia la dirección B."*

La atribución de la dirección a una persona constituye un paso probatorio independiente.

5.5.7 Riesgo de inferencias forenses excesivas

La existencia de:

Numerosas wallets

Operaciones internacionales / P2P

Stablecoins y DeFi

Exchanges extranjeros

No demuestra por sí misma fraude o lavado de activos. Estos elementos pueden incrementar el riesgo de investigación, pero una conclusión pericial debe diferenciar:

operación complejaoperación irregularoperación ilícita

La auditoría forense debe fundamentarse en evidencia y no en la mera complejidad tecnológica del movimiento.

5.5.8 Modelo integrado de riesgo contable-financiero-forense

Para efectos del Manual, puede utilizarse el siguiente modelo conceptual:

- ACTIVO VIRTUAL
- NATURALEZA ECONÓMICA
- CONTROL Y TITULARIDAD
- CLASIFICACIÓN CONTABLE
- MEDICIÓN
- CUSTODIA
- MERCADO / LIQUIDEZ
- CONTRAPARTE
- RIESGO TECNOLÓGICO
- RIESGO REGULATORIO Y TRIBUTARIO
- REGISTRO CONTABLE
- REVELACIÓN
- EVIDENCIA FORENSE

Cada una de estas etapas puede generar una incorrección independiente o interactuar con las restantes.

5.5.9 Mapa de propagación del riesgo

Una característica particularmente importante de los criptoactivos consiste en que un mismo evento puede generar múltiples efectos sucesivos. Por ejemplo:

Hackeo del exchangesuspensión de retiroriesgo de contraparteincertidumbre sobre recuperaciónposible deterioroproblema de liquidezimposibilidad de pagar obligacionesriesgo de negocio en marchanecesidad de revelaciones adicionales.

Por tanto, los riesgos no deberían examinarse como compartimentos independientes.

Tabla No. 7

Riesgos particulares según la modalidad de tenencia

Modalidad	Riesgo predominante
Wallet de autocustodia	Claves y ciberseguridad
Exchange centralizado	Contraparte y custodia
Cold wallet	Pérdida física / acceso
Hot wallet	Ataques cibernéticos
Stablecoin	Emisor, reservas y *depeg*
Staking	Protocolo, bloqueo y precio
Lending	Crédito y liquidación
DEX	*Smart contract* y liquidez
Liquidity pool	*Smart contract* y pérdida económica
Wrapped asset	*Bridge* / custodio
NFT	Liquidez y valoración
Token financiero	Crédito / mercado
RWA tokenizado	Derecho sobre activo subyacente

Esta clasificación demuestra que el riesgo depende tanto del criptoactivo como de la arquitectura mediante la cual se posee o utiliza.

5.5.10 Revelaciones de riesgos financieros

Cuando los criptoactivos calificados como instrumentos financieros entran en juego, la NIIF 7 adquiere especial importancia. La norma exige revelaciones que permitan evaluar la importancia de los instrumentos, la naturaleza y magnitud de los riesgos y cómo fueron administrados (IFRS Foundation, s. f.).

Entre los riesgos definidos por la NIIF 7 se encuentran:

- Riesgo de crédito
- Riesgo de liquidez
- Riesgo de mercado

No obstante, debe evitarse aplicar mecánicamente la NIIF 7 a criptomonedas contabilizadas como intangibles solo porque económicamente presentan riesgos semejantes. Primero debe verificarse el alcance normativo correspondiente.

5.5.1 Evolución regulatoria y riesgo durante 2026

La evaluación debe entenderse dentro de un entorno regulatorio en constante evolución. La revisión del FSB (agosto de 2025) concluyó que persistían brechas significativas respecto de stablecoins, cooperación transfronteriza, recopilación de datos y consistencia de implementación (FSB, 2025). En su programa de trabajo de 2026, el FSB mantiene expresamente el seguimiento de criptoactivos y stablecoins (FSB, 2025/2026). Esto significa que una política de riesgos elaborada para activos virtuales no debería permanecer estática.

5.5.2 Criterio integrador para la evaluación de riesgos

El riesgo relacionado con activos virtuales debe analizarse mediante un enfoque multidimensional que integre:

riesgo contable+ financiero + tecnológico+ operativo + custodia + regulatorio} + tributario + fraude y cumplimiento

Ninguna de estas dimensiones resulta suficiente de manera aislada. Para efectos del presente Manual se propone la siguiente secuencia operativa:

IDENTIFICARATRIBUIRCLASIFICARVALORARCONCILIAREVALUAR RIESGOSOBTENER EVIDENCIAREVELARCONCLUIR

5.5.3 Conclusión del apartado

Los riesgos contables y financieros asociados con los criptoactivos poseen características particulares derivadas de la combinación entre volatilidad económica, infraestructura tecnológica, mercados globales, custodia digital y evolución regulatoria.

Desde la perspectiva forense, el aspecto fundamental consiste en transformar esos riesgos en procedimientos verificables. La evaluación forense debe buscar permanentemente la correspondencia:

realidad económicaregistro contableevidencia documentalevidencia blockchain

Cuando los cuatro componentes resultan coherentes, se incrementa la confiabilidad de la información examinada.

5.6 Revelaciones y notas a estados financieros

La adecuada presentación de información relacionada con criptoactivos no concluye con su reconocimiento y medición. Debido a su naturaleza tecnológica, volatilidad y diversidad contractual, las notas a los estados financieros adquieren especial importancia. La NIC 1 establece que un juego completo de estados financieros incluye notas sobre políticas contables materiales y otra información explicativa (IFRS Foundation, 2024).

5.6.1 La materialidad como criterio rector de las revelaciones

Las NIIF no exigen incorporar en las notas toda la información disponible sobre cada activo. La entidad debe ejercer juicio para identificar aquella información cuya omisión o representación errónea pudiera influir en las decisiones de los usuarios. Las modificaciones a la NIC 1 sustituyeron la exigencia de políticas "significativas" por "información material", evitando notas estandarizadas (IFRS Foundation, 2021).

5.6.2 Pronunciamiento específico del IFRS Interpretations Committee sobre revelaciones

La decisión del IFRS Interpretations Committee de junio de 2019 establece que, además de cualquier otra revelación exigida:

Las criptomonedas tratadas como inventarios deben cumplir los requerimientos de la NIC 2 (párrs. 36-39).

Las tratadas conforme a la NIC 38 deben cumplir los párrafos 118 a 128.

Cuando se midan a valor razonable, aplican los párrafos 91 a 99 de la NIIF 13.

Deben revelarse los juicios de la administración y considerarse los hechos posteriores (NIC 10) (IFRS Interpretations Committee, 2019).

Esquema conceptual de revelación:

clasificación contablenorma aplicablerevelaciones específicasjuiciosincertidumbresriesgohechos posteriores

5.6.1 Identificación clara de los activos virtuales

La primera exigencia práctica consiste en evitar categorías excesivamente agregadas (como "otros activos"). La NIC 1 reconoce que elementos de naturaleza o función diferentes deben presentarse separadamente cuando resulten materiales (IFRS Foundation, 2024). Por ejemplo, un Bitcoin bajo NIC 38 no debe agregarse indiscriminadamente con un token que constituya un instrumento financiero bajo NIIF 9.

5.6.2 Revelación de la política contable aplicada

Las notas deben detallar de manera específica el reconocimiento, clasificación, medición inicial, medición posterior y baja del activo, explicando por qué determinado tratamiento resulta aplicable a las circunstancias concretas de la entidad.

5.6.3 Revelación de juicios contables significativos

La NIC 1 exige revelar los juicios de la administración al aplicar políticas contables con efectos significativos (IFRS Foundation, 2024). Ejemplos materiales: determinar si un activo es inventario o intangible, si existe mercado activo, si se actúa como *broker-trader*, o si un protocolo DeFi representa una transferencia real o un nuevo derecho.

5.6.4 Fuentes de incertidumbre en las estimaciones

La NIC 1 requiere revelar información sobre hipótesis futuras y fuentes principales de incertidumbre de estimación al cierre cuando exista riesgo de ajustes materiales en el ejercicio siguiente (IFRS Foundation, 2024, NIC 1, párr. 125). Debe distinguirse el juicio contable (qué norma aplica) de la incertidumbre de estimación (determinación de importes monetarios).

5.6.5 Revelaciones cuando se aplica la NIC 38

Para criptoactivos bajo la NIC 38, el párrafo 118 exige revelar vidas útiles, métodos de amortización, importes brutos, deterioro acumulado y una conci-

liación entre saldos iniciales y finales (IFRS Foundation, 2021). Dicha conciliación contable de importes no debe confundirse con una relación de movimientos tecnológicos en la blockchain.

5.6.6 Vida útil de criptoactivos clasificados como intangibles

Si el activo intangible posee vida útil finita o indefinida, la NIC 38 requiere revelar las razones que justifican dicha evaluación (IFRS Foundation, 2021, párr. 122). La inexistencia de una fecha contractual de expiración no debe ser el único fundamento en un entorno tecnológico cambiante.

5.6.7 Conciliación del importe en libros

La conciliación exigida por la NIC 38 (párr. 118[e]) puede estructurarse conceptualmente así:

Saldo inicial+ adquisiciones + activos recibidos revaluaciones - disposiciones - deterioros + reversionesotros = Saldo final

5.6.8 Revelaciones sobre revaluación

Cuando se aplique válidamente el modelo de revaluación de la NIC 38, debe sustentarse por referencia a un mercado activo. Las notas deben permitir comprender la fecha efectiva, el importe y la consistencia de la metodología de precios aplicada.

5.6.9 Revelaciones sobre deterioro

Conforme a la NIC 36, una revelación material sobre deterioro debe explicar el evento que originó la evaluación (reducción de precios, desaparición de mercados, abandono de proyectos o vulnerabilidad de protocolos) sin recurrir a descripciones genéricas.

5.6.1 Criptomonedas contabilizadas como inventarios

Cuando aplique la NIC 2, deben revelarse las políticas de medición, fórmula de costo, importes en libros, valor razonable menos costos de venta, deterioros y garantías otorgadas (NIC 2, párr. 36), evitando aplicar notas diseñadas para activos intangibles.

5.6.2 Revelaciones de *broker-traders*

Las entidades que reúnan las condiciones de *broker-trader* bajo la NIC 2 deben revelar el importe de inventarios medidos a valor razonable menos costos de venta (NIC 2, párr. 36[c]), evitando generar la impresión de que todo el inventario opera bajo este régimen.

5.6.3 Revelaciones de valor razonable

Cuando se mida a valor razonable, aplican los requerimientos de la NIIF 13 (párrs. 91-99), permitiendo comprender las técnicas de valoración y datos empleados, dado que un precio visible en internet no implica automáticamente un Nivel 1.

5.6.4 Jerarquía del valor razonable

La NIIF 13 establece tres niveles (Nivel 1: precios cotizados; Nivel 2: datos observables; Nivel 3: datos no observables) (NIIF 13, párr. 72). Su correcta clasificación es crítica ante diferencias en la profundidad y liquidez de los mercados de criptoactivos.

5.6.5 Técnicas de valoración y datos utilizados

Cuando la medición dependa de modelos basados en comparables o flujos económicos (Nivel 2 o 3), la nota debe detallar las hipótesis y la incertidumbre asociada, evitando fórmulas genéricas.

5.6.6 Mercado principal, fuente de precios y hora de valoración

La selección del mercado bajo NIIF 13 no debe basarse en elegir la cotización más favorable. Cuando involucre juicio significativo, se recomienda revelar:
mercado utilizadouente del preciofecha y horazona horariapar de negociación

5.6.7 Revelación cuantitativa de unidades

Para tenencias materiales, es recomendable complementar el importe monetario en la moneda de presentación con las unidades físicas mantenidas (por ejemplo, cantidades de BTC o ETH), facilitando la relación con las variaciones del mercado sin comprometer la materialidad.

5.6.8 Valor de mercado frente al importe en libros

Cuando se utilice el modelo del costo y el valor de mercado difiera significativamente del importe en libros, la información complementaria de mercado puede revelarse claramente diferenciada del importe reconocido bajo NIIF, evitando confusiones contables.

5.6.9 Revelación de custodia y control

Dada la distinción entre autocustodia y custodia de terceros (exchanges especializados), cuando las circunstancias de custodia sean materiales se debe revelar la concentración de riesgo sin exponer nunca datos críticos de seguridad como claves privadas o *seed phrases*.

5.6.10 Activos restringidos, bloqueados o comprometidos

Cuando existan activos en garantía, períodos de bloqueo, staking, depósitos en protocolos o congelamientos administrativos, la información debe distinguir claramente entre la tenencia económica y la disponibilidad efectiva de los recursos.

5.6.11 Hechos ocurridos después del período sobre el que se informa

La volatilidad de los criptoactivos hace especialmente relevante la NIC 10 *Hechos Ocurridos después del Periodo sobre el que se Informa*.

La NIC 10 distingue entre acontecimientos que proporcionan evidencia sobre condiciones existentes al cierre hechos ajustables y aquellos que reflejan condiciones surgidas posteriormente hechos no ajustables. Los primeros afectan los importes reconocidos; los segundos no modifican las cifras de cierre, aunque pueden requerir revelación cuando sean materiales (IFRS Foundation, 2024).

El IFRS Interpretations Committee destacó específicamente que una entidad con criptomonedas debe considerar si las variaciones de valor posteriores al cierre son tan significativas que su falta de revelación pueda influir en las decisiones de los usuarios (IFRS Interpretations Committee, 2019).

Por ejemplo:

31 de diciembre: valor de la tenencia = 10 millones.

15 de enero: caída extraordinaria = valor de 4 millones.

Si la caída refleja circunstancias surgidas después del cierre, normalmente no se modificaría retroactivamente el valor del 31 de diciembre por ese solo acontecimiento; sin embargo, la magnitud de la reducción podría exigir revelar la naturaleza del hecho y su efecto financiero estimado.

La NIC 10 exige precisamente que, para cada categoría material de hechos no ajustables, se revele su naturaleza y una estimación de su efecto financiero o se indique que dicha estimación no puede realizarse (IFRS Foundation, 2024, NIC 10, párr. 21).

5.6.12 Hechos posteriores relacionados con seguridad y custodia

Los eventos posteriores no se limitan a cambios de precios. También puede producirse después del cierre:

- Hackeo de un custodio
- Pérdida de claves
- Insolvencia de un exchange
- Vulneración de un protocolo
- Congelamiento de activos
- Prohibición regulatoria

La entidad deberá determinar si tales acontecimientos proporcionan evidencia acerca de condiciones existentes al cierre o surgieron posteriormente. La evaluación es fundamental porque determina si corresponde:

Ajustar los estados financieros, o

Revelar el evento sin modificar los importes de cierre.

5.6.13 Información comparativa

La utilidad de las notas aumenta cuando permiten comparar la posición de un período con el anterior. La NIC 1 exige información comparativa respecto del período precedente, incluyendo información comparativa en las notas cuando corresponda (IFRS Foundation, 2024).

En consecuencia, cuando existan saldos materiales de criptoactivos, la información debería permitir observar cambios relevantes entre períodos:

Concepto	20X2	20X1
Criptoactivos bajo NIC 38	5,000,000	2,500,000
Criptoactivos bajo NIC 2	1,500,000	800,000
Deterioro acumulado	(600,000)	(200,000)
Activos medidos a valor razonable, cuando corresponda	2,100,000	1,250,000
Total neto	**8,000,000**	**4,350,000**

Nota. Los importes y categorías son exclusivamente ilustrativos; la presentación real deberá adecuarse a las políticas y normas aplicables a cada entidad.

Una evolución material debería explicarse cuando sea necesaria para comprender el período.

5.6.14 Políticas de asignación de costos

Cuando las criptomonedas constituyan inventarios, la NIC 2 exige revelar la política de medición y la fórmula de costo utilizada (IFRS Foundation, 2023, NIC 2, párr. 36[a]).

Este aspecto resulta particularmente relevante cuando existen numerosas adquisiciones del mismo activo a precios diferentes. La nota debería permitir comprender si la entidad utiliza, según resulte permitido:

FIFO, promedio ponderado o identificación específica, dependiendo de la naturaleza de los activos y los requerimientos de la NIC 2.

La fórmula utilizada debe coincidir con la efectivamente aplicada en los registros auxiliares.

5.6.15 Cambios de políticas y estimaciones contables

Los rápidos cambios en el ecosistema cripto pueden motivar modificaciones en determinadas estimaciones o, excepcionalmente, en políticas contables.

La NIC 8 establece los criterios para distinguir cambios en políticas de cambios en estimaciones y regula su tratamiento contable. El IASB introdujo modificaciones destinadas precisamente a facilitar dicha diferenciación (IFRS Foundation, 2021).

En activos virtuales puede producirse, por ejemplo, una revisión de:

Vida útil

Metodología de valoración

Determinada estimación relevante

La entidad deberá determinar si se trata de una nueva información que modifica una estimación o de un verdadero cambio de política. Esta distinción afecta tanto el tratamiento temporal como las revelaciones.

5.6.16 Información tributaria relacionada con criptoactivos

Las notas también deben considerar las consecuencias fiscales de las operaciones cuando resulten relevantes conforme a la NIC 12 y demás normas aplicables. Como se desarrolló en el numeral 5.4, puede existir una diferencia entre el importe contable y la base fiscal.

Una revaluación reconocida contablemente puede no producir inmediatamente un incremento equivalente de la base fiscal, generando potencialmente diferencias temporarias. Asimismo, pueden existir incertidumbres respecto de la interpretación de las normas tributarias aplicables a operaciones con *staking*, minería, *airdrops*, DeFi o intercambios cripto-a-cripto.

La revelación deberá efectuarse conforme al marco tributario y contable aplicable y no mediante afirmaciones genéricas sobre la tributación de los criptoactivos.

5.6.1 Operaciones con partes relacionadas

Los activos virtuales pueden facilitar transferencias directas entre *wallets* controladas por socios, directivos, empresas vinculadas u otras partes relacionadas. Cuando las operaciones satisfagan las condiciones establecidas por la NIC 24, deberán considerarse sus requerimientos de revelación.

Desde una perspectiva forense adquiere particular importancia identificar:

wallet de la entidad → wallet del accionista / directivo / empresa vinculada

La dirección blockchain por sí sola no identifica necesariamente a una parte relacionada; esa vinculación requiere evidencia adicional. Una vez establecida, sin embargo, la operación debe analizarse de acuerdo com su verdadera sustancia económica y los requerimientos correspondientes de información financiera.

5.6.2 Transferencias entre *wallets* propias

No todas las transferencias observables en blockchain requieren revelación como transacciones económicas. Una transferencia:

wallet corporativa A → wallet corporativa B

puede constituir únicamente un cambio de ubicación del mismo activo. En consecuencia, no debe inflarse el volumen de adquisiciones o disposiciones contabilizando transferencias internas como si fueran operaciones con terceros.

No obstante, cuando exista una modificación relevante de la modalidad de custodia por ejemplo, traslado de activos desde autocustodia hacia un custodio externo que origine nuevos riesgos materiales dicha circunstancia puede resultar relevante para las notas aun cuando no exista una venta.

5.6.3 Revelación de activos dados en garantía

Cuando los criptoactivos se utilicen como garantía, la disponibilidad económica del activo puede encontrarse restringida. La NIC 2 exige expresamente revelar el importe de los inventarios dados en garantía de pasivos (IFRS Foundation, 2023, NIC 2, párr. 36[h]). Para activos sometidos a otras normas deberán analizarse los requerimientos específicos correspondientes.

Esta información resulta particularmente importante en estructuras de financiación cripto, donde una caída del valor del colateral puede originar solicitudes adicionales de garantía o liquidaciones automáticas.

5.6.4 Información sobre liquidez

La existencia de activos digitales de elevado valor no necesariamente significa que la entidad posea liquidez equivalente. Un criptoactivo puede encontrarse:

- Bloqueado
- Comprometido
- Depositado en *staking*
- Sujeto a períodos de retiro
- Negociado en mercados poco profundos

Dichas circunstancias sean materiales para comprender la capacidad de la entidad de atender sus obligaciones, las notas deberían proporcionar la información exigida por las normas aplicables. Cuando se trate de instrumentos financieros, la NIIF 7 establece específicamente revelaciones relativas a la naturaleza y extensión del riesgo de liquidez y a su gestión (IFRS Foundation, 2024).

5.6.5 Negocio en marcha

Una exposición material a criptoactivos puede, en situaciones extremas, afectar la evaluación de negocio en marcha. Por ejemplo:

Pérdida sustancial del valor de reservas

Insolvencia de un custodio

Bloqueo de una proporción crítica de activos líquidos

Grandes obligaciones garantizadas mediante criptoactivos

La evaluación debe realizarse conforme a las normas generales aplicables al negocio en marcha. No toda volatilidad justifica una incertidumbre material. Debe analizarse si los acontecimientos afectan efectivamente la capacidad de la entidad para continuar operando.

5.6.6 Revelaciones sobre seguridad: límite entre transparencia y protección del activo

Existe una tensión particular en activos virtuales entre transparencia financiera y seguridad tecnológica. Las notas pueden requerir explicar la modalidad general de custodia, concentración o restricciones; sin embargo, revelar información operacional excesivamente detallada puede generar riesgos adicionales.

Por ello deben evitarse datos como:

- Claves privadas (*private keys*)
- Frases semilla (*seed phrases*)
- Mecanismos exactos de recuperación
- Credenciales de acceso
- Localización física de dispositivos
- Procedimientos internos que permitan eludir controles

La información financiera debe proporcionar transparencia sobre la exposición económica sin comprometer la seguridad del activo.

5.6.7 Información *on-chain* como sustento, no necesariamente como contenido de la nota

Un aspecto especialmente importante para la auditoría forense consiste en distinguir entre:

Información que debe figurar públicamente en la nota, e

Información que debe formar parte de la evidencia que sustenta la nota.

Por ejemplo, no siempre será necesario publicar todos los TxID de las operaciones de una empresa. Sin embargo, los papeles de trabajo deberían permitir vincular:

saldo de la nota → libro mayor → auxiliar → exchange / wallet → transacciones blockchain

Por tanto, la información *on-chain* puede constituir evidencia de respaldo aunque no aparezca detalladamente en los estados financieros.

5.6.8 Conciliación entre notas y evidencia blockchain

Desde la perspectiva del presente Manual, la información revelada debería ser susceptible de reconstrucción mediante la siguiente cadena:

- NOTA A LOS ESTADOS FINANCIEROS ↓
- CUENTA CONTABLE ↓
- LIBRO AUXILIAR DE CRIPTOACTIVOS ↓
- EXCHANGE / CUSTODIO / WALLET ↓
- EVIDENCIA BLOCKCHAIN ↓
- OPERACIÓN ECONÓMICA ORIGINAL

La ausencia de conexión entre estas etapas incrementa el riesgo de que las revelaciones no representen adecuadamente la realidad económica.

5.6.9 Revelaciones sobre incertidumbre regulatoria

Cuando un cambio regulatorio pueda afectar materialmente la capacidad de utilizar, transferir, vender o custodiar determinados criptoactivos, la entidad deberá evaluar si la información correspondiente resulta necesaria para comprender sus estados financieros.

Esto puede adquirir especial relevancia cuando una entidad depende significativamente de:

- Un exchange sujeto a restricciones
- Un token cuya negociación puede ser suspendida
- Una actividad cuyo régimen jurídico se encuentra modificándose

La revelación debe describir condiciones concretas que afecten a la entidad, no realizar una descripción genérica de todas las regulaciones existentes en el mercado.

5.6.10 Revelación de contingencias y procesos legales

Los criptoactivos pueden estar involucrados en:

- Litigios
- Investigaciones regulatorias
- Bloqueos judiciales
- Reclamaciones contra exchanges
- Controversias sobre titularidad
- Procedimientos fiscales

Cuando corresponda, deberán analizarse los requerimientos de la NIC 37 y otras normas aplicables. Desde una perspectiva forense, debe diferenciarse entre activo técnicamente existente y activo jurídicamente disponible. Un criptoactivo puede seguir apareciendo en blockchain, pero encontrarse sujeto a una medida judicial que impida su disposición.

5.6.11 Revelaciones sobre pérdidas por fraude, robo o incidentes tecnológicos

Cuando la entidad haya sufrido una pérdida material por robo, hackeo, fraude o vulneración de un protocolo, el usuario debería poder comprender su efecto cuando las normas aplicables requieran revelarlo. La nota debería diferenciar claramente entre:

Hecho comprobado, frente a

Importe todavía sujeto a recuperación o estimación.

Por ejemplo, una transferencia no autorizada definitivamente comprobada presenta una situación diferente de fondos temporalmente bloqueados en un exchange respecto de los cuales existe una reclamación en curso. Esta distinción resulta crítica para evitar afirmar como pérdida definitiva un importe cuya recuperación todavía se encuentra pendiente o, en sentido contrario, presentar como plenamente recuperable un activo respecto del cual existe incertidumbre material.

5.6.12 Modelo integral de información a revelar

Para una entidad con exposición material a criptoactivos, la estructura de una nota podría organizarse de la siguiente manera:

Componente de la nota	Información principal
Naturaleza	Tipos de criptoactivos y finalidad de tenencia
Clasificación	NIC 38, NIC 2, NIIF 9 u otra norma
Política contable	Reconocimiento, medición y baja
Medición	Costo, revaluación, VNR, valor razonable, según corresponda
Unidades	Cantidades materiales por clase
Importe en libros	Saldo inicial y final
Movimientos	Compras, ventas, deterioros, revaluaciones y otros cambios
Valor razonable	Jerarquía, mercado, técnica e *inputs* cuando resulte aplicable
Vida útil	Finita / indefinida en activos bajo NIC 38
Deterioro	Pérdidas, reversiones y causas
Custodia	Modalidad general y concentración material
Restricciones	Garantías, bloqueos o limitaciones relevantes
Riesgos	Mercado, liquidez, crédito o contraparte según norma aplicable
Juicios	Decisiones contables significativas
Estimaciones	Fuentes materiales de incertidumbre
Tributación	Efectos fiscales relevantes
Hechos posteriores	Cambios o incidentes materiales
Contingencias	Litigios, bloqueos o reclamaciones relevantes

Nota. La matriz constituye una propuesta de sistematización para el presente Manual y no debe interpretarse como un listado obligatorio e indiscriminado de revelaciones. Cada entidad deberá aplicar los requerimientos concretos de las NIIF que correspondan y el principio de materialidad.

5.6.13 Ejemplo ilustrativo de nota sobre criptoactivos

A efectos didácticos, una nota podría estructurarse del siguiente modo:

Nota X – Activos virtuales

La entidad mantiene determinadas criptomonedas principalmente con fines de inversión. Sobre la base de las características económicas de dichas tenencias y de la política contable adoptada, estas se clasifican como activos intangibles conforme a la NIC 38 y se miden posteriormente mediante el modelo del costo. Al cierre del período, el importe en libros de dichas tenencias asciende a X unidades monetarias.

La entidad mantiene asimismo determinados criptoactivos destinados a su venta dentro del curso ordinario de las operaciones, los cuales se contabilizan como inventarios conforme a la NIC 2.

La administración efectúa conciliaciones periódicas entre los registros auxiliares, las cuentas mantenidas en exchanges y las wallets controladas por la entidad. Las tenencias se encuentran distribuidas entre mecanismos de autocustodia y terceros custodios.

La determinación de la clasificación contable y, cuando corresponde, de determinadas mediciones de valor razonable requiere juicio profesional. Las fuentes de precio y mercados utilizados se seleccionan conforme a la política de valoración de la entidad y a los requerimientos de la NIIF 13.

Durante el ejercicio se reconocieron pérdidas por deterioro por X unidades monetarias relacionadas con [describir circunstancias materiales].

Después del cierre se produjo [describir acontecimiento material]. De acuerdo con la NIC 10, el acontecimiento fue considerado [ajustable/no ajustable]. Cuando corresponda, el efecto financiero estimado asciende a X unidades monetarias.

El ejemplo debe adaptarse a los hechos concretos. No debe utilizarse como texto estandarizado para entidades cuyas circunstancias sean diferentes.

5.6.14 Enfoque de auditoría sobre las revelaciones

Desde la perspectiva de auditoría, no basta con comprobar matemáticamente que las cifras de la nota coinciden con el libro mayor. Debe evaluarse también si la revelación es completa, comprensible, neutral, materialmente correcta y consistente con la evidencia disponible.

Por ejemplo, una nota puede indicar correctamente:

“Criptoactivos: 5 millones”

pero resultar incompleta si omite que 4,5 millones se encuentran bloqueados en un exchange sujeto a un procedimiento de insolvencia. En este supuesto, la cifra puede ser aritméticamente correcta, pero la información global proporcionada al usuario podría resultar insuficiente para comprender la verdadera exposición de la entidad.

5.6.15 Enfoque forense sobre las revelaciones

En auditoría forense, las notas adquieren una dimensión adicional porque constituyen declaraciones formales de la administración acerca de la situación de los activos. Por ello, debe verificarse la correspondencia entre:

lo revelado → lo contabilizado → lo documentado
→ lo ocurrido en blockchain

Una divergencia puede representar error, deficiencia de control, omisión, clasificación incorrecta o una situación que requiera investigación adicional. No debe concluirse automáticamente que existe fraude; la metodología forense deberá establecer previamente la naturaleza y causa de la diferencia.

5.6.16 Procedimiento de validación de la nota

Una adecuada revisión de revelaciones sobre criptoactivos debería permitir responder cuatro cuestiones fundamentales:

- **¿Existe?** La evidencia blockchain o del custodio debe sustentar la existencia del activo.
- **¿Pertenece o es controlado por la entidad?** Debe existir evidencia suficiente sobre derechos y control económico.
- **¿Está correctamente valorado?** La metodología debe coincidir con la NIIF aplicable.
- **¿La nota describe adecuadamente la realidad económica y los riesgos materiales?** Las revelaciones deben ser consistentes con los hechos verificados.

Este enfoque evita que el análisis se limite a una comprobación puramente formal de la nota.

5.6.1 Relación entre revelaciones y los numerales anteriores del capítulo

Las notas constituyen el punto de integración de los apartados precedentes:

5.1 Reconocimiento contable: determina qué recurso debe incorporarse.

5.2 Medición y valoración: determina su importe.

5.3 Registro de operaciones: explica cómo los hechos económicos son reflejados en los libros.

5.4 Tributación y fiscalidad: analiza sus consecuencias fiscales.

5.5 Riesgos contables y financieros: identifica las principales exposiciones.

5.6 Revelaciones y notas: proporciona al usuario la información material necesaria.

Así, puede construirse la siguiente secuencia operativa:

RECONOCIMIENTO → MEDICIÓN → REGISTRO → TRIBUTACIÓN → RIESGOS → REVELACIÓN

Una deficiencia en cualquiera de las primeras cinco etapas puede trasladarse directamente hacia la última.

5.6.2 Transición hacia la NIIF 18

Debe incorporarse una precisión normativa especialmente importante para un Manual cuya primera edición corresponde a 2026. El IASB emitió en abril de 2024 la NIIF 18 *Presentación e Información a Revelar en los Estados Financieros*, que sustituirá a la NIC 1. Su aplicación obligatoria comienza para períodos anuales que se inicien a partir del 1 de enero de 2027, permitiéndose su aplicación anticipada (IFRS Foundation, 2024).

Por consiguiente, durante 2026 debe distinguirse entre:

Entidades que continúan aplicando NIC 1, y

Entidades que hayan adoptado anticipadamente NIIF 18, cuando dicha aplicación esté permitida.

La NIIF 18 conserva numerosos principios procedentes de la NIC 1, pero introduce nuevos requerimientos sobre presentación, agregación y desagregación y traslada determinados requerimientos previamente contenidos en la NIC 1 hacia otras normas, entre ellas la NIC 8 y la NIIF 7 (IFRS Foundation, 2024). Esta transición debe ser considerada en futuras ediciones del Manual.

5.6.1 Principio de desagregación

La emisión de la NIIF 18 refuerza además la importancia de la agregación y desagregación adecuada de la información. Este principio resulta particularmente pertinente para los activos virtuales.

Una cuenta denominada:

"Otros activos digitales: 50 millones"

puede ser formalmente compacta, pero económicamente poco informativa si comprende Bitcoin, stablecoins, NFT, tokens financieros y posiciones DeFi sometidos a tratamientos y riesgos totalmente distintos. En consecuencia, la información debe agregarse cuando los elementos compartan características suficientemente similares y desagregarse cuando las diferencias sean materiales para comprender los estados financieros.

5.6.2 Evitar información estandarizada o *boilerplate*

Una nota extensa no es necesariamente una nota adecuada. Existe el riesgo de incorporar páginas completas sobre qué es blockchain, qué es Bitcoin, cómo funciona la minería y qué es una wallet sin explicar qué criptoactivos posee realmente la entidad, cuánto representan, cómo se contabilizan y cuáles son sus riesgos materiales.

Las modificaciones relativas a la revelación de políticas contables buscan precisamente favorecer información específica y material frente a descripciones estandarizadas que pueden oscurecer la información relevante (IFRS Foundation, 2021). Por tanto, una nota de calidad debe ser específica para la entidad.

5.6.3 Consistencia entre las diferentes notas

Las revelaciones relacionadas con criptoactivos pueden encontrarse distribuidas en diferentes partes de los estados financieros: intangibles, inventarios, instrumentos financieros, impuestos, riesgos, hechos posteriores, contingencias y partes relacionadas. Debe existir consistencia entre todas ellas.

Por ejemplo, si la nota de activos intangibles informa 10 millones de criptoactivos, mientras la nota de riesgos declara una exposición total de 15 millones, la diferencia deberá ser explicable por otras categorías contables. Las inconsistencias entre notas constituyen un indicador importante para los procedimientos de auditoría y análisis forense.

5.6.4 Trazabilidad de las revelaciones

Para efectos del presente Manual se propone que toda cifra material revelada respecto de activos virtuales sea susceptible de trazabilidad mediante la siguiente estructura:

ESTADO FINANCIERO ↓
NOTA ↓
CUENTA CONTABLE ↓
MAYOR ↓
AUXILIAR DE CRIPTOACTIVOS ↓
WALLET / EXCHANGE / CUSTODIO ↓
TxID O REGISTRO EQUIVALENTE ↓
DOCUMENTO ECONÓMICO DE ORIGEN

Este modelo permite que la revelación no constituya simplemente una narración preparada al cierre, sino el resultado de un sistema de información verificable.

5.6.5 Matriz de coherencia de las revelaciones

Una revisión forense puede utilizar cuatro niveles de concordancia:

Concordancia cuantitativa: las cifras coinciden entre estados financieros, notas y registros.

Concordancia tecnológica: las unidades y movimientos son compatibles con wallets, exchanges y blockchain.

Concordancia económica: las operaciones reflejan su verdadera sustancia.

Concordancia normativa: el tratamiento y revelación corresponden a la NIIF aplicable.

La existencia de coincidencia matemática sin concordancia económica no es suficiente. Por ejemplo, una wallet puede mostrar exactamente 100 tokens y la contabilidad también 100 tokens, pero si dichos tokens son propiedad de clientes y la entidad actúa únicamente como custodio, el problema no es de cantidad sino de reconocimiento y derechos.

5.6.6 Documentación mínima de respaldo

Los papeles de trabajo utilizados para sustentar una nota material sobre criptoactivos deberían permitir reconstruir, sin necesidad de revelar información de seguridad sensible:

- Naturaleza del activo
- Clasificación contable
- Cantidad y costo
- Importe en libros
- Metodología de valoración y fuente de precios
- Custodia y restricciones
- Movimientos relevantes y deterioros
- Riesgos y hechos posteriores

Esta documentación adquiere especial relevancia cuando la información depende de sistemas externos que pueden posteriormente modificar sus interfaces, desaparecer o restringir el acceso histórico. La conservación sistemática de evidencia incrementa la capacidad de auditoría y reconstrucción forense.

5.6.7 Criterio integrador de revelación

La calidad de las revelaciones sobre activos virtuales puede evaluarse respondiendo sucesivamente:

1. ¿Qué posee la entidad?
2. ¿Qué derechos representa?
3. ¿Cómo se ha clasificado?
4. ¿Cómo se ha medido?
5. ¿Cuál es su importe en libros?
6. ¿Qué cambió durante el período?
7. ¿Dónde y cómo se custodia?
8. ¿Existen restricciones?
9. ¿Cuáles son los juicios y estimaciones materiales?
10. ¿Cuáles riesgos relevantes existen?
11. ¿Han ocurrido acontecimientos materiales después del cierre?
12. ¿Existe evidencia suficiente para respaldar la información presentada?

La respuesta integrada a estas cuestiones permite trasladar la complejidad técnica de los criptoactivos hacia información financiera comprensible.

5.6.8 Criterio contable-forense para las notas

Desde el enfoque de auditoría forense, una nota sobre activos virtuales no debe evaluarse únicamente en función de su cumplimiento formal con una lista de requerimientos. Debe comprobarse simultáneamente la legalidad de la evi-

dencia, la existencia del activo, el control, la integridad, la valoración, la consistencia y la trazabilidad.

La blockchain puede constituir una fuente de evidencia altamente relevante para determinadas afirmaciones, pero no sustituye los contratos, documentos bancarios, registros de exchanges, evidencia de identidad ni demás elementos necesarios para interpretar el hecho económico. Por consiguiente, la robustez de una revelación aumenta cuando existe corroboración entre fuentes independientes.

5.6.9 Conclusión del apartado

Las revelaciones sobre activos virtuales constituyen un componente esencial para lograr una representación comprensible de su efecto sobre la situación financiera, el rendimiento y los riesgos de una entidad. La particular naturaleza de estos activos hace que el importe reconocido en el estado de situación financiera pueda resultar insuficiente si no se acompaña de información sobre su clasificación, política de medición, movimientos, valoración, restricciones, custodia, juicios significativos y acontecimientos posteriores.

El IFRS Interpretations Committee (2019) estableció expresamente que las entidades con tenencias de criptomonedas deben considerar, según corresponda, los requerimientos de revelación de la NIC 2, NIC 38, NIIF 13, NIC 1 y NIC 10, además de cualquier otra información necesaria para comprender los estados financieros.

Para las criptomonedas contabilizadas bajo la NIC 38, adquieren especial importancia las revelaciones sobre vida útil, importe en libros, amortización, deterioro y conciliación de movimientos. Para las mantenidas como inventarios, resultan relevantes la política de medición, fórmula de costo, importes en libros, valor razonable menos costos de venta cuando corresponda, gastos y reducciones de valor (IFRS Foundation, 2023). Cuando la medición se efectúa a valor razonable, la NIIF 13 agrega información sobre la jerarquía de valor razonable y los datos utilizados en la valoración.

Asimismo, las entidades deben revelar los juicios significativos y, cuando corresponda, las fuentes materiales de incertidumbre de estimación que permitan al usuario comprender cómo se determinaron los importes presentados (IFRS Foundation, 2024).

La volatilidad de los criptoactivos hace particularmente relevante la NIC 10. Un cambio material producido después del cierre no necesariamente modifica los importes reconocidos a dicha fecha, pero puede exigir revelar la naturaleza del acontecimiento y su efecto financiero cuando constituya un hecho poste-

rior no ajustable material (IFRS Foundation, 2024; IFRS Interpretations Committee, 2019).

Desde la perspectiva de auditoría forense, la principal exigencia consiste en que cada importe material revelado pueda ser reconstruido y sustentado. En consecuencia, debe existir concordancia entre:

estados financieros → notas → contabilidad → auxiliares → exchanges / custodios → wallets → evidencia blockchain → documentación económica

La revelación constituye, por tanto, el último eslabón de la cadena contable, pero al mismo tiempo se convierte en el primer punto desde el cual un usuario, auditor, regulador o perito puede comenzar a reconstruir la realidad económica de las operaciones.

Finalmente, debe considerarse la evolución normativa inmediata. A la fecha de elaboración de la primera edición 2026 del presente Manual, la NIC 1 continúa siendo relevante para entidades que no hayan aplicado anticipadamente la nueva norma; sin embargo, la NIIF 18 *Presentación e Información a Revelar en los Estados Financieros* será obligatoria para períodos anuales iniciados a partir del 1 de enero de 2027, permitiéndose su aplicación anticipada (IFRS Foundation, 2024). Esta transición deberá considerarse tanto en la aplicación práctica del capítulo como en futuras actualizaciones del Manual.

Este capítulo ha sido elaborado bajo los estándares académicos de la Asociación Interamericana de Contabilidad (AIC). Las posiciones jurídicas sustantivas descansan sobre fuentes primarias verificadas: instrumentos legislativos vigentes de la República Dominicana, reglamentaciones europeas, estándares del GAFI, la OCDE y el CIAT, precedentes judiciales federales de los Estados Unidos y doctrina institucional del Ministerio Público Fiscal argentino (UFECI).

En aras del principio de trazabilidad de fuentes propio de la auditoría forense, se advierte al lector que en secciones específicas particularmente 6.1, 6.3, 6.4, 6.7 y 6.8 se ha incorporado doctrina técnica proveniente de portales especializados de acceso abierto (*digitalperito.es*, *beltsys.com*, *victifin.org*, *datawallet.com*, *ethereum.org*, *metlabs.io*), cuyo contenido se identifica en el aparato bibliográfico como «fuente web especializada». Estas referencias han sido cotejadas contra la doctrina consolidada y deberán ser verificadas por la Comisión Técnica de Peritaje Contable y Auditoría Forense de la AIC durante la revisión editorial final. Las referencias del CIAT y de los organismos multilaterales (GAFI, OCDE, BIS, FinCEN, UFECI) tienen carácter institucional consolidado y no requieren la misma cautela editorial.

Todas las abreviaturas y anglicismos técnicos se explican mediante notas al pie en lenguaje sencillo, atendiendo al mandato de accesibilidad práctica del Manuals.

6 RIESGOS JURÍDICOS Y DELITOS ASOCIADOS

6.1 Lavado de activos con criptoactivos

El Lavado de Activos («Money Laundering») ejecutado mediante criptoactivos mantiene las tres fases clásicas de la tipología tradicional colocación, estratificación e integración, pero adquiere dinámicas de hipervelocidad y complejidad técnica en entornos on-chain y off-chain. El Boletín núm. 111 del Banco de Pagos Interamerican Es («BIS»), publicado en 2025, propone precisamente aprovechar la transparencia natural de las cadenas públicas asignando un *puntaje de riesgo AML* a cada dirección de billetera con base en su trayectoria transaccional, invirtiendo el paradigma de dependencia exclusiva de intermediarios.

Mecanismos y tipologías forenses principales

1. Mezcladores y bóvedas de privacidad («*Crypto Mixers & Tumblers*»): protocolos como Tornado Cash o Blender.io agrupan los fondos de múltiples usuarios para romper el vínculo criptográfico e histórico entre las direcciones de origen y destino. El auditor forense debe identificar interacciones con estos contratos inteligentes mediante heurísticas de análisis de grafos, evaluando patrones de depósito y retiro temporalmente correlacionados.
2. Monedas enfocadas en la privacidad («*Privacy Coins*»): criptoactivos como Monero (XMR) o Zcash (ZEC) que utilizan criptografía avanzada firmas de anillo, direcciones furtivas y pruebas de conocimiento cero o *zk-SNARKs* para ocultar sistemáticamente al emisor, al receptor y el monto transaccionado.
3. Saltos entre cadenas («*Chain Hopping*») y puentes («*Cross-Chain Bridges*»): táctica consistente en mover rápidamente capitales de una blockchain a otra (por ejemplo, de Bitcoin a Ethereum y luego a Avalanche) empleando exchanges descentralizados («DEX») o puentes no custodiados, con el objeto de confundir a los programas de trazabilidad lineal.
4. Mulas de dinero digitales y servicios «P2P»: uso de cuentas de terceros en intercambios locales o plataformas «peer-to-peer» no reguladas para liquidar grandes volúmenes de criptoactivos a moneda fíat («cash-

out»), fraccionando los montos por debajo de los umbrales obligatorios de reporte («ROS/STR»).

Marco de referencia Interamericana para el auditor

- Recomendación 15 del GAFI («FATF R.15»): aplicable a las Nuevas Tecnologías y a los Proveedores de Servicios de Activos Virtuales («PSAV / VASP»).
- La Regla de Viaje («Travel Rule»): exige a los PSAV obtener, retener y transmitir la información del originador y del beneficiario en transacciones que superen el umbral estándar (usualmente USD 1,000).
- Reglamento MiCA y TFR (Unión Europea): consolidan la Regla de Viaje para criptoactivos y establecen la licencia obligatoria de CASP para operar dentro del Espacio Económico Europeo.

En el ámbito iberoamericano, el auditor forense debe familiarizarse con las herramientas de trazabilidad utilizadas por firmas especializadas —Chainalysis Reactor, Elliptic Investigator, TRM Labs y CipherTrace—, cuya lógica opera sobre heurísticas de agrupamiento («*clustering*»), análisis de flujo por grafo dirigido y contraste contra listas de sanciones OFAC/SDN.

6.2 Financiamiento del terrorismo

A diferencia del lavado de activos cuyo objetivo final es legalizar el origen ilícito del capital, el Financiamiento del Terrorismo (FT) busca ocultar el *destino* de los fondos, con independencia de si el capital de origen es lícito (donaciones, organizaciones no gubernamentales) o ilícito.

Metodologías de captación y movilización

- Micro-mecenazgo y campañas de crowdfunding descentralizado: difusión de direcciones públicas de billeteras en canales de mensajería cifrada (Telegram, Signal) solicitando aportes en stablecoins de baja volatilidad (USDT, USDC) para el sostenimiento de células logísticas.
- Redes de remesas informales («*Hawala Digital*»): corredores que liquidan transacciones de criptoactivos en fronteras o zonas de conflicto donde el sistema bancario tradicional es inexistente o está severamente bloqueado.

Fuentes de inteligencia y listas de sanciones («Sanctions Screening»)

El auditor forense encargado de peritajes relacionados con FT debe cruzar obligatoriamente las direcciones on-chain investigadas con las listas negras actualizadas de:

1. OFAC (Office of Foreign Assets Control del Departamento del Tesoro de los EE. UU.), específicamente la lista SDN (Specially Designated Nationals).
2. Consejo de Seguridad de las Naciones Unidas (CSNU): resoluciones relativas a sanciones y congelamiento de activos conexos al terrorismo y la proliferación de armas de destrucción masiva.
3. Listas locales: en la República Dominicana, las emitidas por el Comité Nacional Contra el Lavado de Activos (CONCLA); en Paraguay, las de la SEPRELAD.

La doctrina de la Unidad Fiscal Especializada en Ciberdelincuencia («UFECI») del Ministerio Público Fiscal de la República Argentina, expuesta en su *Informe sobre Criptoactivos* (mayo de 2023), constituye un referente regional. La UFECI destaca la especial relevancia de las stablecoins centralizadas en la ecuación FT, dado que sus emisores (Tether Limited y Circle) han demostrado capacidad técnica y voluntad regulatoria de congelar direcciones incluidas en listas OFAC mediante la función *addToBlacklist* incorporada en los contratos inteligentes de emisión.

6.3 Fraudes financieros y estafas digitales

La ingeniería social combinada con la falta de cultura financiera y tecnológica del usuario promedio propicia esquemas de defraudación masiva. El Informe UFECI (2023) advierte que, en jurisdicciones latinoamericanas, el fraude cripto ya representa la primera causa de denuncia por ciberdelito patrimonial, superando el *phishing* bancario tradicional.

Modalidades críticas

- Envenenamiento de direcciones («*Address Poisoning*»): los atacantes generan una dirección de billetera que coincide exactamente con los primeros y últimos caracteres de la billetera legítima de la víctima. Envían una transacción de valor cero para que quede registrada en el historial; cuando la víctima copia la dirección de su última transacción para un envío futuro, transfiere los fondos al defraudador.
- Estafas de afecto o engaño romántico («*Pig Butchering*» / «*Sha Zhu Pan*»): organizaciones criminales estructuradas establecen relaciones de confianza a largo plazo con las víctimas por redes sociales, persuadiéndolas de invertir grandes sumas en plataformas de trading falsas que simulan rendimientos extraordinarios antes de bloquear los retiros.
- Suplantación de identidad («Phishing») y malware de portapapeles («*Crypto Clippers*»): software malicioso que detecta cuándo el usuario

copia una dirección alfanumérica y la reemplaza silenciosamente en el portapapeles por la del delincuente al momento de pegar.

- Falsos «*airdrops*» y sitios espejo: réplicas fraudulentas de sitios web oficiales que solicitan la conexión de la billetera del usuario mediante una firma que, en realidad, autoriza el vaciado total de sus activos.

Circular SB Núm. 016/22: régimen dominicano de advertencias

La Circular SB Núm. 016/22 de la Superintendencia de Bancos de la República Dominicana institucionaliza el mecanismo de *Circulares de Advertencia* contra esquemas de intermediación financiera o cambiaria no autorizada, incluyendo aquellos con componentes tecnológicos potencialmente fraudulentos. La circular consagra una política de *tolerancia cero* respecto a las entidades supervisadas que faciliten productos o servicios a operadores de dichos esquemas, calificando la conducta como infracción Muy Grave bajo el literal (a) numeral 14 del artículo 68 de la Ley Monetaria y Financiera (Ley núm. 183-02).

6.4 Esquemas Ponzi y rug pull

En el ecosistema cripto, las pirámides financieras tradicionales y los fraudes técnicos coexisten, amparados bajo la promesa de altos rendimientos garantizados («*yield farming* extremo»).

Esquemas Ponzi cripto

Estructuras piramidales o esquemas multinivel (MLM) disfrazados de fondos de arbitraje con Inteligencia Artificial o minería en la nube. El pago de retornos a los inversionistas antiguos se financia estrictamente con el ingreso de las aportaciones de nuevos inversionistas. El auditor forense demuestra el delito evidenciando la ausencia de una actividad económica real subyacente en los flujos de caja y analizando el comportamiento de dispersión en la blockchain.

Caso paradigmático 2025: *United States v. Do Kwon* (Distrito Sur de Nueva York, agosto de 2025). Do Kwon, fundador de Terraform Labs, se declaró culpable ante la justicia federal estadounidense por dos cargos conspiración para defraudar y fraude electrónico vinculados al colapso en 2022 del ecosistema TerraUSD/Luna, con pérdidas estimadas de USD 40,000 millones. El acuerdo con la Fiscalía Federal de Manhattan contempla renuncia a activos por más de USD 19 millones y sentencia máxima de 25 años, fijada para el 11 de diciembre de 2025. Este precedente confirma la posibilidad efectiva de imputación penal a fundadores de proyectos DeFi por representaciones fraudulentas realizadas ante inversionistas.

Tirón de alfombra («Rug Pull»)

Fraude propio del ámbito de las Finanzas Descentralizadas («DeFi») donde los desarrolladores de un nuevo proyecto captan capital masivo de inversionistas para proveer liquidez y, repentinamente, abandonan el proyecto vaciando los fondos del pozo de liquidez («*Liquidity Pool*»). Las subtipologías se sintetizan en el cuadro siguiente:

Subtipología de Rug Pull	Mecanismo técnico	Detección forense
Extracción de liquidez *(«Liquidity Stealing»)*	El creador retira los pares de tokens depositados en el contrato AMM (Automated Market Maker).	Verificar si los LP Tokens fueron quemados o bloqueados («time-locked») en un contrato inteligente de custodia temporal.
Pote de miel *(«Honeypot»)*	El contrato inteligente incluye código malicioso que permite comprar el token, pero prohíbe la venta a cualquier dirección ajena a la lista blanca del creador.	Auditoría del código fuente en Solidity; búsqueda de funciones ocultas que modifican tarifas de transferencia al 100 %.
Venta masiva de desarrolladores *(«Hard/Soft Rug»)*	Los creadores retienen el 50 % o más del suministro en billeteras no declaradas y venden masivamente al mercado, desplomando el precio a cero.	Análisis de distribución inicial de tokens y mapeo de clústeres de billeteras interconectadas.
Manipulación de oráculo	Ataque de préstamo relámpago («flash loan») que distorsiona el precio del oráculo utilizado por el protocolo, permitiendo drenar fondos a precio artificial.	Correlación de bloques del ataque con transacciones de préstamo relámpago; auditoría de la lógica del oráculo del protocolo.

Auditoría de contratos inteligentes: buenas prácticas

De acuerdo con la documentación oficial del ecosistema Ethereum y con la doctrina técnica publicada por firmas especializadas en auditoría de smart contracts, la mitigación de riesgo en proyectos DeFi contempla al menos los siguientes controles que el auditor forense debe verificar como diligencia mínima:

- Auditoría independiente del código por firmas reputadas (CertiK, OpenZeppelin, Trail of Bits, Consensys Diligence, Halborn, Quantstamp).
- Bloqueo temporal («time-lock») de las funciones administrativas de emergencia.
- Renuncia («renounce ownership») a las funciones privilegiadas de acuñación y modificación de comisiones.
- Publicación del código fuente verificado en un explorador de bloques (Etherscan, BscScan).

- Uso de oráculos descentralizados de reputación (Chainlink, Pyth) frente a oráculos de fuente única.
- Programas activos de recompensa por hallazgo de vulnerabilidades («bug bounty»).

6.5 Evasión tributaria y ocultamiento patrimonial

El seudo-anonimato y la autocustodia («*self-custody*») en billeteras frías o de hardware permiten a los contribuyentes ocultar bases imponibles a las administraciones tributarias.

Modalidades de ocultamiento fiscal

- Falta de declaración de hechos imponibles: omisión de reporte de ganancias de capital en operaciones de permuta cripto-cripto, rendimientos de staking, minería de confirmación bajo mecanismos PoW o PoS, y recepción de airdrops.
- Deslocalización ficticia: simulación de residencia fiscal en jurisdicciones de nula o baja tributación cripto mediante el uso de redes privadas virtuales («VPN») y corporaciones extraterritoriales («offshore») que actúan como tenedoras de activos virtuales.
- Uso indebido del régimen de amnistía: en la República Dominicana, la Ley 30-26 concede una ventana de amnistía fiscal hasta el 31/12/2026 (Art. 8). El abuso de esta amnistía para regularizar ganancias cripto de origen posiblemente ilícito debe activar alertas al auditor forense sobre la eventual configuración concurrente de lavado de activos.

Doctrina CIAT (2026): tres rasgos estructurales de la tributación directa de criptoactivos

Alfredo Collosa, en publicación del Centro Interamericano de Administraciones Tributarias (CIAT, 18 de agosto de 2026), sistematiza tres rasgos estructurales que hacen a los criptoactivos irreductibles a las categorías tributarias tradicionales y que el auditor forense debe considerar como marco conceptual de todo dictamen fiscal en la materia:

1. Descentralización: los criptoactivos no están emitidos ni respaldados por ningún banco central ni autoridad pública; su registro se mantiene de forma distribuida entre los nodos de una red, sin que exista una entidad central que pueda informar automáticamente a las administraciones tributarias, como sí ocurre con las entidades financieras tradicionales bajo los estándares FATCA o CRS.
2. Transnacionalidad nativa: una misma operación puede iniciarse, ejecutarse y liquidarse sin que en ningún momento intervenga un sujeto esta-

blecido en el país de residencia del contribuyente, lo que dificulta enormemente la aplicación de los criterios tradicionales de territorialidad y de localización de la fuente de renta.

3. Heterogeneidad funcional: bajo la etiqueta «criptoactivo» conviven instrumentos con funciones económicas radicalmente distintos medios de pago, instrumentos de inversión, fichas de acceso a servicios («*utility tokens*»), representaciones tokenizadas de activos físicos o financieros, lo que impide aplicar una única regla de tributación transversal.

Como consecuencia, la mayoría de los países ha optado por una *aproximación pragmática por analogía*, aplicando a los criptoactivos las reglas existentes para bienes de naturaleza jurídica similar. Esta opción aporta continuidad y seguridad jurídica relativa, pero traslada al intérprete contribuyente, asesor o administración tributaria la carga de decidir, caso por caso, con qué figura tradicional se asimila cada operación concreta. La calificación jurídica es entonces determinante de la carga fiscal.

Bifurcación de la calificación jurídica según el CIAT

La mayor parte de los países considera los criptoactivos una forma de *propiedad*, pero dentro de esa categoría general las soluciones se bifurcan en cuatro grandes vías:

- Activos intangibles (mayoría de las jurisdicciones): tratamiento asimilable al de propiedad inmaterial gravable por ganancia de capital. Es la vía adoptada por la Ley 30-26 dominicana (Art. 19 → Art. 289 CT) y por la doctrina de la DIAN colombiana.
- Commodities o mercaderías: posición sostenida en los EE. UU. por la CFTC respecto de Bitcoin y Ether, generando régimen de ganancia de capital ordinaria.
- Instrumentos financieros: aplicable cuando el token en cuestión reproduce derechos económicos propios de un valor negociable («security tokens»); en tal caso se equipará a acciones o bonos y suele tributar bajo régimen de valor mobiliario.
- Vías radicalmente distintas: Italia asimila las monedas virtuales a divisas extranjeras a determinados efectos; Polonia las califica legalmente como «representación digital de valor» sin mayor precisión; El Salvador y la República Centroafricana confirieron al Bitcoin la condición de moneda de curso legal, con las consecuencias fiscales que ello comporta al equipararlo, a efectos prácticos, al resto de operaciones en moneda nacional.

El problema estructural del IRNR y los convenios de doble imposición

El Impuesto sobre la Renta de No Residentes («IRNR») plantea en el caso de los criptoactivos un problema estructural: al no existir un soporte físico iden-

tificable los activos se registran en la blockchain, no en un dispositivo con ubicación geográfica, resulta necesario acuñar un *criterio artificial de localización* para poder aplicar las reglas de sujeción al impuesto.

La Dirección General de Tributos («DGT») de España resolvió esta cuestión en la Consulta Vinculante V1069-19, fijando como criterio de localización *el lugar donde radique la entidad que presta el servicio de custodia de las claves criptográficas privadas*. Este criterio, aún de aplicación discutida, es el más citado en la doctrina iberoamericana como referente interpretativo cuando el legislador nacional no ha regulado expresamente la localización de los criptoactivos.

A esta dificultad se suma la ausencia de mención expresa a los criptoactivos en los convenios de doble imposición («CDI») vigentes, lo que obliga a encajar las rentas derivadas de estas operaciones en las cláusulas de reparto ya existentes (rentas empresariales, ganancias de capital, dividendos, intereses o cánones, según el caso). El resultado es un mosaico de soluciones nacionales que genera dos riesgos simétricos y opuestos que el auditor forense debe documentar:

- Doble imposición: cuando dos Estados reclaman gravar la misma renta bajo criterios de localización distintos (por ejemplo, país de residencia del titular versus país de radicación del custodio de claves).
- Doble no imposición: cuando la operación no es alcanzada por ninguna de las jurisdicciones involucradas por defecto o incompatibilidad de sus reglas de conexión, generando arbitraje fiscal.

El Estándar CARF de la OCDE y la Directiva DAC 8 de la UE

Para combatir la opacidad fiscal, la OCDE desarrolló el CARF y la Unión Europea aprobó la Directiva DAC 8 (octava enmienda a la Directiva 2011/16/UE). Ambos instrumentos, cuyo primer intercambio de información está previsto para el año 2027, obligan a exchanges, brokers y determinadas plataformas descentralizadas a identificar a sus usuarios y reportar automáticamente sus operaciones a las administraciones tributarias de los países de residencia. Se prevé que este marco reduzca sustancialmente el margen de infradeclaración que hasta ahora ha caracterizado al mercado cripto, complementando las enmiendas al *Common Reporting Standard* («CRS 2.0») que ahora captura también las stablecoins y los activos digitales sujetos a custodia por PSAV.

Ley núm. 30-26 de la República Dominicana: reconocimiento del criptoactivo como activo de capital

La Ley núm. 30-26 del 18 de junio de 2026, «de medidas pro-crecimiento económico, simplificación fiscal y mitigación de la crisis Interamericana», sitúa a la República Dominicana en la vía mayoritaria descrita por el CIAT criptoactivo como activo intangible sujeto a ganancia de capital:

- Artículo 19 de la Ley 30-26 → Artículo 289 del Código Tributario: redefine *activo de capital* como todo bien «incluyendo bienes digitales y criptoactivos». El criptoactivo pasa a ser expresamente activo de capital, cuyas enajenaciones generan ganancia de capital gravable.
- Artículo 12 de la Ley 30-26 → Artículo 269 del Código Tributario: instaura un régimen de *renta mundial atenuada* que grava a residentes por rentas de fuente extranjera provenientes de inversiones y ganancias financieras, alcanzando las utilidades obtenidas en exchanges del exterior.
- Tasa aplicable: 27 % para personas jurídicas (Art. 297 CT) y escala progresiva para personas físicas (Art. 296 CT). El 10 % único y definitivo del nuevo Art. 296-1 CT está limitado a ganancias de capital inmobiliarias de personas físicas y no aplica al cripto, salvo debate interpretativo aún abierto en materia de tokenización inmobiliaria.

Vacíos que persisten y que el auditor forense debe documentar como riesgo alto en sus dictámenes conforme al marco conceptual del CIAT: (i) método de costeo obligatorio (FIFO versus costo promedio); (ii) momento de realización en permutas cripto-cripto; (iii) regla de conversión a peso dominicano («DOP») a la fecha de operación; (iv) tratamiento fiscal de las recompensas de minería y staking; (v) criterio de localización para efectos del IRNR ante la ausencia de doctrina administrativa dominicana análoga a la Consulta DGT V1069-19 española. Estos vacíos deben cubrirse en el reglamento de la eventual Ley de Activos Digitales y Criptoactivos, actualmente en fase de anteproyecto ante la Cámara de Diputados (Oficio 05569 del 09/04/2026).

6.6 Ciberdelito y criptoactivos

Los criptoactivos operan como combustible financiero de la ciberdelincuencia moderna al permitir el cobro seguro y extorsivo de rescates.

1. Secuestro de datos («*Ransomware*»): ataques a infraestructuras gubernamentales y corporativas que cifran bases de datos críticas. El rescate se exige casi universalmente en Bitcoin (BTC) o Monero (XMR). Metodológicamente, los peritos forenses analizan las notas de rescate, extraen las direcciones públicas y aplican vigilancia automatizada («address watch») en los exploradores de bloques para detectar el momento exacto en que los fondos comienzan a moverse hacia los nodos de lavado.
2. Criptopiratería («*Cryptojacking*»): uso no autorizado de la potencia de procesamiento («CPU/GPU») de servidores, computadoras o dispositi-

vos IoT de víctimas para minar criptomonedas de forma oculta, consumiendo electricidad y desgastando el hardware corporativo en beneficio del atacante.

3. Robo de credenciales y drenaje de billeteras: ataques dirigidos contra las claves privadas o frases semilla del usuario mediante «phishing» avanzado, ingeniería social o malware. La evidencia forense se localiza en el análisis de las transacciones de barrido («sweep transactions») que consolidan los fondos hacia una dirección receptora del atacante.
4. Ataques al ecosistema DeFi: explotación de vulnerabilidades en contratos inteligentes mediante préstamos relámpago («flash loans»), reentrada («reentrancy»), manipulación de oráculos o desbordamientos aritméticos. El precedente de Chainalysis 2026 registra que estos ataques han superado en volumen a los robos a exchanges centralizados desde 2023.

La instrumentación forense recomendada por FinCEN en su Aviso 2025 sobre *Ransomware and Financial System Facilitation* contempla, como mínimo: (a) preservación inmediata de la cadena de custodia digital; (b) recolección de artefactos forenses del sistema comprometido (memoria RAM, registros de eventos, notas de rescate); (c) coordinación temprana con la unidad de inteligencia financiera nacional; (d) evaluación previa de la licitud del pago del rescate bajo el régimen de sanciones aplicable a la jurisdicción.

6.7 Extinción de dominio y recuperación de activos digitales

La incautación de activos virtuales presenta desafíos procedimentales e informáticos sin precedentes para fiscales, jueces y auxiliares de justicia. La doctrina desarrollada por la UFECI argentina y Colombia han adelantado guías procedimentales para la afectación de los bienes en el proceso penal y de extinción de dominio y por firmas especializadas en peritaje forense cripto identifica cuatro fases metodológicas:

FASE 1: Identificación y trazabilidad (on-chain)

Uso de exploradores públicos y software heurístico de agrupamiento («clustering») Reactor de Chainalysis.

FASE 2: Vinculación física (off-chain)

Requerimiento judicial KYC/AML al PSAV / Exchange de salida – solicitud de comiso y perdida del poder dispositivo dentro del proceso penal o dentro del un proceso administrativo de extinción de dominio resolución de medidas cautelares de congelamiento.

FASE 3: Medida cautelar / congelamiento

Blacklist en USDT/USDC o congelamiento en cuenta del exchange – aplicación de solicitudes

FASE 4: Incautación y traslado a custodia judicial

Reasignación a billetera fría multifirma del Estado / Ministerio Público – Fiscalía General de la Nación, o sus entidades para la administración de bienes incautados – o su equivalente para la administración de bienes con aplicación de medidas cautelares de extinción de dominio que en Colombia es la sociedad de Activos Especiales SAE.

El proceso técnico de incautación y custodia judicial

1. **Identificación y atribución**: la trazabilidad en la blockchain revela rutas, pero las direcciones son alfanuméricas. La atribución física se logra identificando el punto de contacto con el dinero fíat (generalmente un exchange centralizado o PSAV). Se emite una orden judicial de requerimiento de información KYC / AML a la plataforma para conocer el nombre, documento de identidad, IP y cuentas bancarias asociadas al titular.
2. **Congelamiento de emergencia («Freezing Order»)**: en tokens emitidos de forma centralizada (USDT de Tether o USDC de Circle), las autoridades competentes pueden ordenar directamente al emisor que ejecute una función en el contrato inteligente para colocar en lista negra («*Blacklist*») la billetera infractora, inmovilizando los fondos instantáneamente sin requerir la clave privada del criminal.
3. **Incautación de claves privadas y dispositivos**: cuando los activos están en billeteras autocustodiadas, el decomiso físico requiere el allanamiento y aseguramiento de dispositivos de almacenamiento, hardware wallets (Ledger, Trezor, Coldcard) o el hallazgo de la frase semilla —mnemotécnica (conjunto de técnicas y estrategias mentales para facilitar y acelerar la memorización de información) de 12 a 24 palabras— escrita en papel o soportes metálicos.
4. **Bóvedas judiciales y subasta de activos**: bajo ningún concepto los activos virtuales incautados deben permanecer en las billeteras de los investigados o de los peritos. Los tribunales u organismos de administración de bienes incautados deben transferir los tokens a una billetera fría multifirma («*Multisig Cold Wallet*») del Estado, custodiada institucionalmente hasta la sentencia definitiva de Extinción de Dominio o Decomiso, procediendo eventualmente a su liquidación mediante subasta pública transparente.

Herramientas profesionales de análisis forense

La doctrina técnica especializada identifica el siguiente ecosistema de herramientas profesionales, cuya utilización por parte del auditor forense debe documentarse en el capítulo metodológico del informe pericial:

- **Chainalysis Reactor / KYT**: herramienta hegemónica de investigación y monitoreo AML on-chain. Utilizada por más de 70 unidades de inteligencia financiera en el mundo y de equipos de investigación en cripto activos.
- **Elliptic Investigator / Navigator**: análisis forense y clasificación de direcciones por categoría de riesgo.
- **TRM Labs**: trazabilidad multi-cadena con énfasis en delitos cross-chain y bridges.
- **CipherTrace (Mastercard)**: análisis de riesgo integrado a la infraestructura de tarjetas de pago.
- **Merkle Science**: inteligencia predictiva de comportamiento cripto y análisis de contratos DeFi.
- **Exploradores públicos**: Etherscan, BscScan, Blockchain.com, Solscan y Mempool.space, como fuentes primarias de evidencia gratuita y verificables.

6.8 Normatividad comparada por países

A continuación se presenta el mapa normativo iberoamericano e Interamericana actualizado a agosto de 2026 sobre el estatus jurídico, fiscal y penal de los criptoactivos. La fila correspondiente a la República Dominicana se destaca en color ámbar para reflejar la novedad de la Ley 30-26 y el carácter de anteproyecto de la ley cripto sectorial. La columna de calificación fiscal ha sido conciliada con las cuatro vías identificadas por la doctrina CIAT (2026).

Como ilustración del principio de *heterogeneidad funcional* que Collosa (CIAT, 2026) atribuye a los criptoactivos, resulta especialmente elocuente el contraste entre dos jurisdicciones vecinas de tradición jurídica próxima: mientras la República Dominicana ya consagró por vía legislativa (Ley 30-26 de junio de 2026) el estatus del criptoactivo como activo de capital gravable con arquitectura institucional sectorial en construcción vía anteproyecto, Perú mantiene un proyecto de ley marco (N° 1042/2021-CR) sin aprobación plenaria y una doctrina SUNAT no consolidada, aunque ha sido diligente en incorporar a los PSAV como sujetos obligados AML/CFT desde el Decreto Supremo N° 006-2023-JUS. Ambos modelos son legítimos y responden a decisiones de política fiscal soberana; para el auditor forense actuante en cada jurisdicción, la dife-

rencia se traduce en el *grado de seguridad jurídica documental* con que puede fundamentar su dictamen tributario.

País / Región	Marco normativo principal	Enfoque regulatorio y fiscal	Estatus jurídico de criptoactivos
Unión Europea	Reglamento MiCA (UE) 2023/1114, Reglamento TFR (UE) 2023/1113 y Directiva DAC 8.	Pleno vigor (2024-2026). Licencia obligatoria CASP para operar. Estrictas normativas de PLA/FT y respaldo de stablecoins. DAC 8 inicia intercambios fiscales en 2027.	Valores transaccionables / activos intangibles regulados.
Estados Unidos	SEC, CFTC, FinCEN, OCC y normativas estatales (BitLicense de NY). Guidance Fed 2025 sobre bancos custodios.	Regulación por aplicación coercitiva («enforcement»). Debate legal entre securities y commodities. Fed autorizó a bancos custodiar cripto y ofrecer stablecoins (2025).	Propiedad / títulos valores o commodities según tipología técnica.
El Salvador	Ley Bitcoin (Decreto Legislativo N° 57) y Ley de Emisión de Activos Digitales.	Vía radical (CIAT): Bitcoin como moneda de curso legal. Exención de impuestos sobre la ganancia de capital para BTC. CNAD como órgano rector.	Moneda de curso legal (Bitcoin) / activos digitales (otros).
Brasil	Marco Legal de Criptoactivos (Ley 14.478/2022) e Instrucción Normativa RFB 1888.	El Banco Central de Brasil es el ente regulador. Obligación mensual de reportar transacciones en exchanges locales y extranjeros a la Receita Federal. Tipificación agravada del fraude cripto.	Bienes intangibles transaccionales / activos de inversión.
Argentina	Ley del Impuesto a las Ganancias (LIG), Ley 27.739 de PLA/FT (2024), Resolución CNV 994/2024 y doctrina UFECI del MPF.	Los PSAV están registrados ante la CNV y son sujetos obligados ante la UIF. Las ganancias por enajenación de «monedas digitales» se asimilan a rentas de fuente por valores mobiliarios (alícuota 15 % o 5 %).	Moneda digital equiparada a valor mobiliario para efectos fiscales.
México	Ley Fintech (2018) y regulaciones del Banco de México (Circulares 4/2019).	Los criptoactivos son «activos virtuales». Las Instituciones de Tecnología Financiera («ITF») requieren autorización de la CNBV. Prohibición de oferta directa al público por parte de bancos.	Activos virtuales; no son moneda de curso legal.

Colombia	Concepto DIAN 001357/2019 y doctrina consolidada 100192467-2847 de 2022s. Documento de orientación técnica No. 20	La DIAN considera los criptoactivos como activos intangibles susceptibles de gravamen sobre las ganancias por enajenación. Proyecto de ley cripto en debates. CRIPTOACTIVOS GESTIÓN CONTABLE EN COLOMBIA	Activo intangible / bien inmaterial gravable.
Paraguay	Proyecto de Ley de Criptominería y Resolución SEPRELAD N° 314/21.	Enfoque primordial en la regulación eléctrica y fiscal de la criptominería intensiva. Sujetos obligados en materia de PLA/FT ante la SEPRELAD.	Activos de valor digital no monetario.
Perú	Ley N° 27693 (marco AML/CFT); Ley N° 29038/2007 (incorpora UIF-Perú a la SBS); Decreto Supremo N° 006-2023-JUS (PSAV como sujetos obligados); Resolución SBS N° 02648-2024; Proyecto de Ley N° 1042/2021-CR («Ley Marco de Comercialización de Criptoactivos»), pendiente de aprobación plenaria a mayo de 2026.	Los PSAV están inscritos ante la SBS/UIF como sujetos obligados AML/CFT. No existe licencia sectorial específica ni sandbox regulatorio. La SUNAT considera las rentas de criptoactivos gravables por Impuesto a la Renta, sin doctrina fiscal consolidada. Los security tokens quedan bajo competencia de la SMV.	Bien intangible sin categoría fiscal específica; security tokens sujetos a la Ley del Mercado de Valores.
España	Ley 10/2010 de PLA/FT (mod. Real Decreto-ley 7/2021), Ley del IRPF, Consulta DGT V1069-19 y adecuación al Reglamento MiCA y DAC 8.	Criterio de localización de la Consulta V1069-19: el lugar donde radique la entidad que presta el servicio de custodia de claves privadas. Régimen de ganancia patrimonial en IRPF y sujeción al IRNR para no residentes.	Bien inmaterial computable como ganancia patrimonial.
República Dominicana	Ley núm. 30-26 (18/06/2026) reformando el Código Tributario; Anteproyecto de Ley de Activos Digitales y Criptoactivos (Of. 05569, 09/04/2026); Circular SB Núm. 016/22; Ley 155-17 contra el Lavado de Activos; avisos oficiales BCRD (2017-2024).	Vía mayoritaria CIAT (activo intangible): Ley 30-26 reconoce al criptoactivo como activo de capital (Art. 289 CT). Tributa al 27 % (PJ) o escala progresiva (PF). Amnistía fiscal hasta 31/12/2026. El anteproyecto crea el Consejo Nacional y designa a la SIMV como órgano rector, con PSAD como sujetos obligados AML/CFT.	Activo de capital gravable (Ley 30-26); no es moneda de curso legal (art. 6 del anteproyecto).

La fila de la República Dominicana refleja un marco en tránsito: la sustancia fiscal ya está consolidada por la Ley 30-26, ubicando al país en la *vía mayoritaria CIAT* (calificación como activo intangible generador de ganancia de capital), pero la arquitectura institucional sectorial depende de la aprobación definitiva del anteproyecto. Se recomienda al auditor forense actuante en jurisdicción dominicana citar como fundamento normativo primario la Ley 30-26 y sus reformas al Código Tributario; el anteproyecto solo puede citarse en carácter prospectivo, identificándolo como tal en el dictamen.

PARTE III.

Auditoría Forense Aplicada A Criptoactivos

7 FUNDAMENTOS DE AUDITORÍA FORENSE EN BLOCKCHAIN

La transformación digital de las operaciones económicas ha modificado profundamente la forma en que se producen, almacenan y examinan las evidencias en una investigación financiera. Dentro de este escenario, la tecnología *blockchain* adquiere especial relevancia al permitir registrar transacciones en estructuras distribuidas, vinculadas mediante mecanismos criptográficos y diseñadas para hacer evidentes o resistentes las alteraciones posteriores. Esta característica ofrece nuevas posibilidades para reconstruir movimientos de activos, aunque también plantea desafíos complejos relacionados con la identificación de los usuarios, la preservación de la evidencia y la interpretación técnica de las operaciones (Yaga et al., 2018).

En jurisdicciones que aún carecen de una legislación específica sobre la recolección de evidencia digital en cadenas de bloques, el sustento técnico y probatorio debe construirse integrando la normativa procesal penal sobre prueba y pericia, la ley de delitos informáticos, los marcos de prevención de lavado de activos, la protección de datos y, de manera primordial, la regulación aplicable a los Proveedores de Servicios de Activos Virtuales (PSAV).

La auditoría forense aplicada a *blockchain* surge de la convergencia entre conocimientos contables, financieros, tecnológicos y jurídicos. Su finalidad no es únicamente localizar una transacción digital, sino determinar su significado económico, reconstruir su recorrido y obtener evidencia técnicamente sustentable con validez probatoria ante instancias judiciales, administrativas o de gobierno corporativo.

7.1 Concepto y alcance de la auditoría forense en blockchain

La auditoría forense en *blockchain* se define como la aplicación de procedimientos especializados destinados a identificar, recopilar, preservar, analizar y explicar información financiera y digital registrada en un registro distribuido,

cuando esta contribuya al esclarecimiento de operaciones presuntamente irregulares.

El alcance de esta disciplina comprende:

- La verificación de la existencia, titularidad y control de billeteras y activos digitales.
- La reconstrucción de flujos de fondos entre direcciones públicas (*tracing*).
- La valoración económica de los activos en controversia bajo normas contables aplicables.
- El soporte técnico-probatorio en procesos judiciales, arbitrales o corporativos.

A diferencia de la auditoría financiera tradicional, la evidencia primaria —el registro de transacciones— es pública, inmutable y verificable de forma independiente. No obstante, **el auditor debe observar un límite técnico fundamental**: *identificar una dirección blockchain no equivale necesariamente a identificar a su titular*. Toda evidencia *on-chain* debe contrastarse y complementarse rigurosamente con fuentes *off-chain* (estados bancarios, registros de exchanges, KYC, contratos y declaraciones fiscales).

7.2 Perfil del auditor forense especializado

El entorno de los activos virtuales exige ampliar el perfil tradicional del auditor forense. El profesional debe dominar tres dimensiones clave:

Contabilidad y finanzas forenses: Comprensión de flujos de caja, valoración de activos y detección de anomalías patrimoniales.

Informática y tecnología DLT: Conocimiento de arquitecturas *blockchain*, mecanismos de consenso (PoW/PoS), contratos inteligentes y funcionamiento de billeteras custodiales/no custodiales.

Marco regulatorio ALD/FT y normativo: Dominio de estándares internacionales (GAFI, Regla de Viaje) y leyes penales/tributarias locales.

Una competencia crítica es la distinción entre *trazabilidad* y *atribución*: el perito puede demostrar técnicamente la transferencia de fondos entre direcciones, pero atribuir dichas direcciones a personas físicas o jurídicas exige elementos de corroboración adicionales, evitando extralimitar las conclusiones objetivas de los datos.

7.3 Principios éticos y cadena de custodia digital

La utilidad de una investigación forense depende tanto de la calidad del análisis como de la integridad de la evidencia que lo sustenta. La validez de cualquier hallazgo depende de que la evidencia digital haya sido manejada conforme a un protocolo de cadena de custodia verificable, para lo cual existen directrices Internacionales para la identificación, recolección, adquisición y preservación de evidencia digital, plenamente aplicables a la evidencia proveniente de billeteras, exchanges y nodos de blockchain.

Los principios éticos que deben regir la actuación del auditor forense incluyen los siguientes:

Integridad: documentar cada actuación de forma que sea reproducible por un tercero independiente.

Objetividad: abstenerse de formular conclusiones antes de agotar el análisis técnico de la evidencia disponible; la presión por encontrar elementos incriminatorios no puede sustituir el análisis imparcial de los hechos.

Confidencialidad: proteger la información sensible de las partes, incluidas claves privadas y datos personales asociados a direcciones identificadas.

Competencia profesional y debido cuidado: reconocer los límites del propio conocimiento técnico y recurrir a peritos especializados cuando sea necesario.

La cadena de custodia digital constituye, en este contexto, un mecanismo esencial para documentar la identificación, obtención, transferencia, almacenamiento y análisis de la evidencia. Debe permitir conocer quién obtuvo la información, cuándo fue recogida, qué procedimiento se empleó, dónde fue almacenada y quién tuvo acceso a ella, en armonía con la normativa procesal penal y los procedimientos de cadena de custodia establecidos por las autoridades competentes.

Es importante advertir que la inmutabilidad atribuida a blockchain no reemplaza la cadena de custodia: aunque la transacción permanezca registrada en la red, el auditor debe demostrar cómo obtuvo esa información y cómo preservó los archivos, reportes o registros utilizados para sustentar sus conclusiones. El valor probatorio de una investigación forense puede verse comprometido si no se documenta con precisión la metodología empleada para atribuir direcciones a personas o entidades, dado que dicha atribución rara vez es absoluta y suele basarse en inferencias estadísticas. Por ello, la cadena de custodia digital debe registrar no solo la evidencia en sí (capturas de pantalla, exportaciones de datos, valores hash de verificación), sino también el razonamiento metodológico que sustenta cada conclusión.

7.4 Obtención y preservación de evidencia digital

La obtención de evidencia digital debe responder a procedimientos que garanticen autenticidad, integridad, trazabilidad y reproducibilidad. El proceso comprende cuatro etapas secuenciales, que aplicadas al contexto de criptoactivos se traducen de la siguiente manera:

Identificación: localización de las fuentes de evidencia potencialmente relevantes (direcciones públicas, archivos de billeteras, registros de exchanges, dispositivos móviles o de escritorio, correos electrónicos y comunicaciones relacionadas con la operación).

Recolección: captura de la información sin alterar su estado original, utilizando herramientas que generen un valor hash de verificación (por ejemplo, SHA-256) para acreditar la integridad del archivo capturado.

Adquisición: obtención de copias forenses de dispositivos o bases de datos, empleando bloqueadores de escritura y procedimientos que impidan la modificación de metadatos; el auditor debe diferenciar la fuente original de las copias utilizadas para el análisis.

Preservación: almacenamiento seguro y trazable de la evidencia, con control de acceso y registro de cada persona que la haya consultado o manipulado.

En blockchain, la evidencia puede comprender el identificador de la transacción (TXID), direcciones de origen y destino, fecha y hora, bloque, cantidad transferida, tipo de activo y comisiones, así como las operaciones posteriores realizadas desde la dirección receptora. Esta información debe complementarse con evidencia externa cuando sea necesario establecer la identidad de los participantes o determinar la naturaleza económica de la operación (movimientos bancarios, registros de un proveedor de servicios de activos virtuales, documentación empresarial o información contable).

En el caso específico de billeteras de criptoactivos, la obtención de evidencia exige particular cuidado con las llaves privadas y las frases semilla, pues su exposición indebida podría comprometer la integridad del propio activo objeto de investigación. Se recomienda mantener un registro exhaustivo de cada consulta realizada a exploradores de bloques y herramientas de análisis, incluyendo la fecha, la fuente y la versión del software utilizado, de manera que el proceso sea auditable y replicable por un perito independiente.

La obtención de evidencia tiene, además, límites jurídicos: la normativa sobre delitos informáticos protege los datos y sistemas informáticos frente a determinadas formas de acceso ilícito. En consecuencia, una investigación forense no habilita al profesional para acceder sin autorización a dispositivos, cuentas, billeteras o sistemas; la evidencia debe obtenerse por medios legíti-

mos y respetando las competencias de las autoridades cuando la investigación se desarrolle dentro de un proceso penal.

7.5 Trazabilidad financiera en blockchain y recolección de evidencia digital de la transacción

Una de las particularidades más relevantes de la auditoría forense aplicada a criptoactivos es que, a diferencia de los sistemas bancarios tradicionales, el registro de transacciones en blockchain es público y permanente. La trazabilidad constituye uno de los principales aportes de blockchain a la investigación financiera y consiste en reconstruir, dentro de las posibilidades técnicas de cada red, la secuencia seguida por un activo desde una dirección de origen hacia una o varias direcciones posteriores.

Una investigación puede comenzar con una dirección vinculada al caso. A partir de ella se identifican las transacciones relevantes, sus TXID, montos, fechas y direcciones receptoras, y posteriormente se reconstruyen los movimientos sucesivos hasta localizar puntos de interés, como un exchange, un servicio de intercambio, otra blockchain o una dirección respecto de la cual exista información adicional. La secuencia básica puede expresarse de la siguiente manera:

Wallet de origen TXID, wallet receptora, wallets intermedias, exchange o plataforma, conversión o disposición final del activo.

Esta labor exige del auditor el dominio de técnicas de análisis de grafos y agrupamiento de direcciones (clustering). El avance de las herramientas de analítica de blockchain, incluidas aquellas basadas en inteligencia artificial, ha mejorado sustancialmente la capacidad de vincular direcciones públicas con entidades identificables, aunque persisten limitaciones frente a tecnologías que priorizan la privacidad, como los mezcladores de transacciones, las monedas de privacidad y ciertos protocolos de finanzas descentralizadas. La denominada Regla de Viaje obliga a los proveedores de servicios de activos virtuales a compartir información sobre el originador y el beneficiario de las transferencias que superen determinado umbral, lo cual constituye una fuente adicional de trazabilidad cuando la operación involucra exchanges regulados.

El auditor forense debe documentar con precisión la ruta seguida por los fondos, identificando los puntos de entrada y salida hacia el sistema financiero tradicional (on/off ramps), usualmente representados por exchanges centralizados, dado que estos puntos constituyen la vía más efectiva para vincular activos virtuales con identidades reales.

Sin embargo, la trazabilidad técnica no debe confundirse con una conclusión sobre responsabilidad. El hecho de que determinados activos hayan llegado a una dirección demuestra el movimiento registrado, pero no necesariamente quién controlaba dicha dirección ni cuál fue la finalidad de la operación. El valor del trabajo forense surge precisamente de correlacionar el recorrido digital con evidencia financiera, contable y documental independiente.

7.6 Gestión del riesgo en auditoría de activos virtuales

La gestión del riesgo en auditorías forenses de criptoactivos debe enmarcarse en un modelo integral de administración de riesgo empresarial que vincule la identificación y valoración de riesgos con la estrategia y el desempeño de la organización, y sustentarse en un enfoque basado en riesgos: la utilización de criptomonedas o blockchain no constituye, por sí misma, evidencia de una actividad ilícita.

Entre los riesgos específicos que debe valorar el auditor forense en este campo se encuentran los siguientes:

Riesgo de custodia: pérdida, robo o compromiso de llaves privadas, que puede resultar en la pérdida irreversible del activo.

Riesgo regulatorio: cambios en el marco normativo aplicable a los activos virtuales, que pueden alterar la calificación jurídica del activo o las obligaciones de las partes.

Riesgo de valuación: alta volatilidad de precios, que dificulta la determinación del valor razonable del activo en la fecha relevante para la controversia.

Riesgo de lavado de activos y financiamiento del terrorismo, frente al cual se recomienda un enfoque basado en riesgo que gradúe las medidas de diligencia según el perfil del cliente y de la operación.

Riesgo tecnológico, asociado a vulnerabilidades de los protocolos, contratos inteligentes o plataformas involucradas.

El análisis debe identificar circunstancias objetivas que incrementen la exposición al fraude, lavado de activos, financiamiento del terrorismo u otros riesgos. Entre los factores que requieren mayor atención se encuentran el fraccionamiento de operaciones, movimientos sucesivos entre numerosas direcciones, transacciones entre distintas blockchain, operaciones peer-to-peer, la utilización de mecanismos que dificultan la trazabilidad, la interacción con jurisdicciones de mayor riesgo y movimientos cuya magnitud no guarda relación razonable con el perfil económico conocido del usuario.

El Grupo de Acción Financiera Interamericana sostiene que los países y proveedores de servicios de activos virtuales deben identificar, evaluar y mitigar

los riesgos de lavado de activos y financiamiento del terrorismo asociados con estas actividades (Financial Action Task Force [FATF], 2021). Este criterio resulta especialmente pertinente para la auditoría forense: el riesgo debe evaluarse atendiendo al contexto, comportamiento transaccional y evidencia disponible, evitando considerar sospechosa una operación únicamente por haberse realizado mediante activos virtuales.

La incorporación de los proveedores de servicios de activos virtuales al sistema de prevención del lavado de activos y financiamiento del terrorismo y su sujeción a la supervisión de la autoridad financiera competente constituyen avances relevantes en distintas jurisdicciones. En consecuencia, el auditor debe integrar el análisis tecnológico con los procedimientos de conocimiento del cliente, origen de fondos, perfil transaccional y evaluación de operaciones inusuales, adoptando un enfoque de gestión de riesgo alineado con estándares Internacionales de control interno y de auditoría que permita priorizar recursos hacia las áreas de mayor exposición, documentar adecuadamente el apetito de riesgo asumido por la organización y comunicar de forma clara a la junta directiva las implicaciones de cada hallazgo.

8 METODOLOGÍAS DE AUDITORÍA FORENSE EN BLOCKCHAIN

La auditoría forense aplicada a criptoactivos no constituye una disciplina independiente de la auditoría forense tradicional. Por el contrario, representa una evolución metodológica que incorpora nuevas fuentes de evidencia, nuevos riesgos y nuevas tecnologías dentro del proceso de investigación financiera, patrimonial, contable y digital.

En este contexto, la presente metodología adopta los principios históricos promovidos por la Asociación Interamericana de Contabilidad (AIC) en materia de auditoría forense, complementándolos con técnicas de análisis blockchain, inteligencia financiera, análisis de datos, fuentes abiertas e informática forense.

El modelo propuesto reconoce que el objetivo principal no es rastrear transacciones, sino reconstruir hechos económicos, identificar beneficiarios finales, determinar responsabilidades y documentar evidencia técnicamente sustentada para procesos administrativos, disciplinarios, fiscales, civiles, penales y de recuperación de activos, convirtiendo este tipo de análisis en una documentación técnica contable de la trazabilidad de los activos de valor entre responsables de direcciones de billeteras, bien sea por la identificación biográfica o kyc del proveedor de activos virtuales o por la identificación de responsabilidad transaccional al momento del análisis, como lo sería un análisis de gas, es una metodología de trazabilidad que permite identificar el primer depósito de la moneda nativa, el cual es un indicador de potencial controlador común entre la dirección de origen a la dirección de destino. Donde toma prioridad la primera transacción recibida de TRX, ya que para realizar cualquier transacción con la red de Tron requiere tener fondos en la moneda nativa para hacer frente al pago de comisiones. Es por eso que la primera transacción se toma como proveniente de un potencial controlador por su interés en la activación de la dirección receptora.

Algunas de estas metodologías, siempre están en continuos cambios, toda vez que estas deben comprender y adaptarse a los modelos de negocios, los procedimientos en la identificación, búsqueda y recolección de EMP y EF e

Información Legal Obtenida u otros hallazgos de otros tipos de auditoría, necesarios para la construcción de criterios para la planeación necesaria.

8.1 Planeación de auditoría forense cripto

La planeación debe incluir, personal, equipo interdisciplinario, presupuesto y otros costos de verificar del 100% de los elementos. Incluyendo su procesamiento, análisis y almacenamiento.

Principio Rector AIC

La auditoría forense inicia con la formulación de una hipótesis de investigación y no con la revisión indiscriminada de información, la recolección de evidencia y otros elementos deben corresponder al criterio de hipótesis.

Por ello, la fase de planeación busca responder:

1. ¿Qué hecho requiere ser verificado?
2. ¿Qué riesgo se pretende evaluar?
3. ¿Qué recursos digitales podrían haber sido utilizados?
4. ¿Qué evidencia será necesaria para demostrar o descartar la hipótesis?

Modelo H5 de Planeación Forense Digital

H1. Hecho

¿Qué ocurrió? Identificar cual sería la posible inferencia razonable de delito.

Ejemplos:

- Fraude financiero.
- Lavado de activos.
- Corrupción.
- Soborno.
- Evasión tributaria.
- Apropiación indebida de activos digitales.

H2. Huella

- ¿Qué rastros dejó el hecho?
- Direcciones blockchain.
- Exchanges.
- Registros contables.
- Contratos inteligentes.
- Reportes tributarios.
- Ubicación IP

H3. Holder

- ¿Quién ejercía control económico?
- No basta identificar una wallet, hay que hallar el responsable del dominio o capacidad de transferencia u operación.
- La auditoría debe establecer:
- Control efectivo.
- Beneficiario final.
- Relación patrimonial.

H4. Hub

- ¿Qué intermediarios participaron?
- Exchanges.
- Custodios.
- Protocolos DeFi.
- Marketplaces NFT.
- Pasarelas de pago.
- Puentes

H5. Heritage

- ¿Qué patrimonio fue afectado?
- Activos virtuales.
- Cuentas bancarias.
- Inversiones.
- Bienes muebles.
- Bienes inmuebles.

8.2 Identificación de riesgos y tipologías

Riesgos de Auditoría en Activos Digitales

Riesgo de Existencia

El activo reportado no existe.

Riesgo de Titularidad

El investigado niega el control económico o se encuentra en una estructura anónima.

Riesgo de Integridad

Existe manipulación de registros, el proceso de KYC ineficiente, documentos de identificación falso.

Riesgo de Ocultamiento

Uso de mecanismos tecnológicos para dificultar la trazabilidad.

Riesgo de Valoración

Diferencias significativas derivadas de la volatilidad.

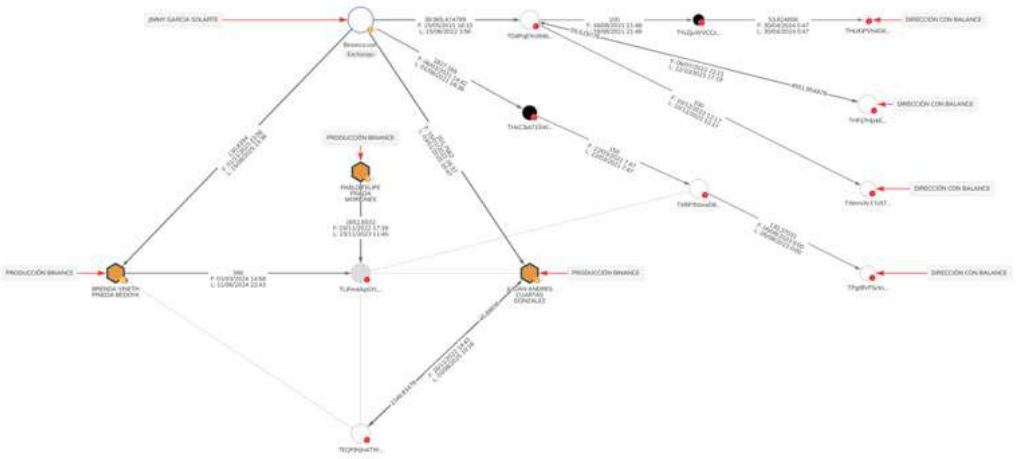
8.3 Técnicas de análisis blockchain

Partiendo de que los análisis de esta información deben ser contrastadas con otras realidades económicas y materiales, como lo es la monetización y como sea de forma inicial las billeteras digitales deben ser cargadas, estas variables son importantes, el comprender que el valor cargado dentro de una billetera a la final pertenece a una persona natural o jurídica y con este, otros comportamientos financieros y económicos que deberán ser reflejados al momento de la identificación e individualización de los comportamientos del modelo de negocio por el cual se utilizan las tecnologías. Se comparan blockchain, estados financieros, declaraciones tributarias, productos financieros y otras evidencias contractuales así todo se realiza, realizando cruces que se validaran más adelante.

Seguidamente hay que preparar la información para una validación mediante una reconstrucción cronológica desde la adquisición, custodia, transferencias de valor, conversiones tanto a las diversas divisas como el comportamiento entre las cripto y la disposición final de los diversos beneficios.

Igualmente, al procesar parte de la información hasta su totalidad con la ayuda de diversas herramientas tecnológicas, se deberá comprender una relación lógica entre la adquisición de valor, del dinero fiat, los bienes muebles e inmuebles o bienes físicos y la conformación de compañías y/o empresas, así como la identificación de las actividades económicas con las cuales están configuradas y sus responsabilidades tributarias de acuerdo a la jurisdicción de su ubicación u operación.

Una de las mejores recomendaciones para comprender la relación de conectividad transaccional es mediante graficas de nodos de correlación a fin de que estos permitan la visualización del flujo de los activos de valor así como la línea de tiempo de las diversas transferencias, al momento de realizar análisis del flujo de monedas nativas estas pueden presentar contraflujos, por lo que lo mejor son los análisis mediante graficas.



Fuente: Diseño propio, con el fin de evidenciar análisis de flujos dentro de la blockchain con diversas direcciones de billeteras.

Este tipo de estructuras graficas, permiten de forma más cómoda la explicación del comportamiento de valor líneas de tiempo y demás actividades propias del análisis. Elemento esencial para la explicación en audiencia sobre el entendimiento del comportamiento y los análisis.

8.4 Rastreo y seguimiento de transacciones

Para el rastreo es de vital importancia identificar con exactitud la fecha y hora de la ocurrencia. En el dictamen o informe pericial se deberá documentar el código alfanumérico completo de la dirección de billetera de origen (por ejemplo, en Bitcoin: bc1qar0srrr7xfkvy5l643lydnw9re59gtzzwf5mdq; o en Ethereum: 0xdB055877e6c13b6A6B25aBcAA29B393777dD0a73), el **hash de** transacción o identificador alfanumérico que certifica la operación (por ejemplo: 0x4e3a3754410177e6937ef1f84bba68ea139e8d1a2258c5f85db9f1cd715a1bdd), así como la dirección de billetera receptora final.

Sincronización horaria (UTC): Todas las transacciones dentro de una red *blockchain* ocurren en una unidad de tiempo universal coordinada (**UTC – 0**), el estándar horario internacional que permite sincronizar las operaciones a nivel mundial (idéntico al tiempo aeronáutico de los pilotos). El perito debe ajustar la hora visible en la red sumando o restando el huso horario correspondiente a la jurisdicción donde se originó o recibió la operación, dato que se corrobora mediante la dirección IP asociada.

El rol de la Dirección IP: Toda transacción con activos virtuales requiere una conexión a Internet (desde redes fijas o móviles, privadas o públicas), lo que genera un registro interno de dirección IP. A pesar de la existencia de contramedidas tecnológicas orientadas al enmascaramiento, la IP constituye un elemento cardinal para ubicar temporal y espacialmente al actor.

El análisis debe determinar fehacientemente hacia dónde se movilizaron los recursos, dónde se encuentran en la actualidad y si fueron monetizados (*cash-out*). Estos datos metodológicos conformarán la matriz base del **Anexo No. 1** del dictamen pericial.

8.5 Identificación de mixers y tumbler services

Durante la reconstrucción de los hechos, el auditor debe determinar si se emplearon tecnologías de anonimización y si su uso respondió a una finalidad legítima o a un propósito deliberado de ocultamiento patrimonial. Dentro del ecosistema se identifican servicios que, aunque lícitos en su concepción técnica, pueden ser instrumentalizados para la fragmentación en operaciones de lavado de activos (tales como *CoinJoin*, *Tumblers*, *Privacy Chains*, criptomonedas centradas en la privacidad como *Monero*, protocolos como *Tornado Cash*, o puentes intercadena reiterativos). Su presencia representa un factor de alto riesgo que exige un análisis forense exhaustivo para evaluar el grado de instrumentalización ilícita.

8.6 Análisis OSINT y fuentes abiertas

Las capacidades de auditoría forense moderna integran herramientas tecnológicas orientadas a procesar grandes volúmenes transaccionales y plataformas de reconocimiento en fuentes abiertas (*OSINT*). Esto permite recuperar datos públicos (correos electrónicos, números de teléfono, nombres, perfiles fotográficos, registros mercantiles o licencias) que los titulares de las direcciones de billeteras hayan expuesto en redes sociales o registros accesibles en internet, facilitando la conexión entre el mundo *on-chain* y las personas naturales o jurídicas investigadas.

8.7 Integración con informática forense

La recolección de evidencia digital exige un rigor extremo no solo en la cadena de bloques, sino también en el tratamiento de los datos biográficos obtenidos de exchanges, las descargas de exploradores y los dispositivos incautados (teléfonos inteligentes, computadoras, tabletas). La extracción de información de estos dispositivos debe realizarse bajo protocolos estrictos de informática forense (uso de bloqueadores de escritura y cálculo de funciones hash SHA-256), garantizando que los elementos no sean alterados y conserven su autenticidad plena ante los tribunales.

9 PROCEDIMIENTOS DE INVESTIGACIÓN FINANCIERA DIGITAL

Introducción del capítulo

La expansión de los criptoactivos y el desarrollo de tecnologías basadas en *blockchain* han transformado significativamente la dinámica de los mercados financieros y los sistemas de pago a escala global. La descentralización y la verificabilidad criptográfica ofrecen nuevas oportunidades para la innovación, pero incrementan la complejidad de las investigaciones sobre delitos económicos (Arriola, 2024).

A diferencia de las investigaciones financieras convencionales —sustentadas en libros contables físicos o extractos bancarios tradicionales, el análisis de criptoactivos demanda la identificación, preservación y análisis de evidencia digital distribuida en redes *blockchain*, plataformas de intercambio (*exchanges*), billeteras digitales (*wallets*), contratos inteligentes y protocolos DeFi (Moreira Mero et al., 2024).

En atención a los estándares internacionales promovidos por el Grupo de Acción Financiera Internacional (FATF, 2026), el presente capítulo desarrolla una metodología estructurada de investigación financiera digital organizada en etapas secuenciales, diseñada para guiar al auditor forense bajo un enfoque basado en riesgos.

9.1 Recolección de información financiera digital

Objetivo

Identificar, obtener, preservar y documentar de forma íntegra toda la información digital potencialmente relevante (activos virtuales, plataformas, billeteras, dispositivos y registros transaccionales), asegurando que los datos sean suficientes, pertinentes, confiables y verificables para sustentar el análisis pericial y su admisibilidad jurídica.

Fundamento técnico

La calidad de una investigación forense descansa en su fase inicial. Aunque las transacciones en *blockchain* son públicas en numerosas redes, su atribución a sujetos específicos requiere integrar fuentes internas y externas (registros

contables, documentación financiera, informes KYC/AML de Proveedores de Servicios de Activos Virtuales - PSAV/VASP, y registros de autenticación). La obtención de evidencia suficiente y adecuada sigue siendo un principio rector de la auditoría (IAASB, 2022).

Procedimientos operativos

Definir el alcance de la investigación: Delimitar los hechos, período analizado, activos involucrados y jurisdicciones competentes.

Identificar las fuentes de información: Registros contables, estados financieros, CEX, DEX, *wallets* frías y calientes, exploradores de bloques y contratos inteligentes.

Obtener información documental y digital: Contratos, facturas, reportes KYC/AML, hashes de transacciones, archivos exportados en CSV, bases de datos y copias forenses de dispositivos.

Preservar la integridad de la información: Registrar marcas temporales (fecha y hora), identificar fuentes, calcular valores hash (SHA-256) y mantener estrictas copias maestras y de trabajo bajo cadena de custodia.

Clasificar la naturaleza económica y tecnológica del activo digital: El auditor no debe basarse únicamente en la denominación comercial, sino evaluar los derechos económicos, mecanismo de emisión, red, contratos inteligentes y posibilidad de rescate (criptoactivos nativos, *stablecoins*, tokens de utilidad/gobernanza, NFT, *wrapped tokens*, posiciones DeFi y activos del mundo real tokenizados - RWA).

Herramientas recomendadas

- *Exploradores Blockchain:* Blockchain.com, Etherscan, BscScan, Tronscan, Solscan.
- *Plataformas de Analytics:* Chainalysis Reactor, TRM Labs, Elliptic Investigator, Crystal Blockchain.
- *Informática Forense y Preservación:* FTK, EnCase, Autopsy, Magnet AXIOM, calculadoras HASH (SHA-256), bloqueadores de escritura.
- *Análisis Financiero:* Microsoft Excel, Power BI, i2 Analyst's Notebook, Maltego.

Riesgos frecuentes y Papeles de trabajo

Riesgos: Obtención incompleta, pérdida de evidencia, fallas en la cadena de custodia, confusión entre custodios y beneficiarios finales, o dependencia de una única fuente.

Papeles de trabajo requeridos: Programa de recolección, inventario de fuentes, registro de *wallets* e inventario de *exchanges*, matriz de información obtenida, actas de recolección, bitácoras de cálculo hash y formularios de cadena de custodia.

9.2 Matrices de riesgo y señales de alerta (*Red Flags*)

Objetivo

Identificar, analizar y valorar los riesgos asociados a operaciones con criptoactivos mediante matrices estructuradas y señales de alerta, priorizando las líneas de investigación según probabilidad e impacto para detectar tempranamente indicios de lavado de activos, financiamiento del terrorismo, fraude o evasión tributaria.

Fundamento técnico

Conforme a las directrices de FATF (2023), los activos virtuales y los VASP deben evaluarse mediante un enfoque basado en riesgos (*Risk-Based Approach*), considerando el perfil del cliente, la naturaleza de las transacciones, los productos empleados y las jurisdicciones involucradas.

Procedimientos y Factores de Riesgo

Identificación de factores: Cliente, beneficiario final, tipo de activo virtual, VASP, jurisdicción, volumen/frecuencia y riesgo tecnológico.

Análisis transaccional: Montos, periodicidad, dispersión entre múltiples billeteras, fragmentación (*smurfing*), saltos entre cadenas (*cross-chain bridges*) y conversión acelerada a fiduciario.

Elaboración de la matriz de riesgo: Cuantificación del riesgo inherente, evaluación de controles vigentes, determinación del riesgo residual y establecimiento de prioridades de investigación.

Catálogo de señales de alerta (*Red Flags*):

- Creación masiva y reiterada de billeteras de reciente data.
- Transferencias sucesivas encadenadas sin justificación económica aparente.
- Interacción con mezcladores (*mixers*) o protocolos de privacidad.
- Operaciones incompatibles con el perfil económico conocido del investigado.
- Recepción de fondos desde direcciones previamente fichadas en listas de sanciones o vinculadas a ilícitos.

9.3 Perfilamiento transaccional

Objetivo

Analizar sistemáticamente el comportamiento transaccional en criptoactivos para identificar patrones, relaciones económicas, anomalías e indicadores de actividades ilícitas, reconstruyendo la lógica financiera y orientando la identificación del beneficiario final.

Procedimientos operativos

Consolidación y ordenamiento cronológico: Integración de todas las transacciones verificando su integridad y clasificándolas por red y tipo de activo.

Análisis del flujo financiero y patrones: Determinación del origen y destino de los fondos, ciclos repetitivos, permanencia en billeteras y conversión entre criptoactivos y dinero fiduciario.

Identificación de operaciones atípicas: Fragmentación (*smurfing*), movimientos circulares, transferencias en cadena y uso intensivo de pasarelas de anonimización.

Valuación económica y reconstrucción patrimonial: Cuantificación rigurosa del valor económico transferido, conservado o transformado, documentando la fecha, hora, red, valor de mercado (con fuentes de cotización verificables), comisiones de red (*gas fees*) y rendimientos generados por *staking*, *lending* o *liquidity pools*.

Conciliación blockchain-contabilidad-tributación: Confrontación sistemática de la evidencia digital con los registros contables, estados financieros y declaraciones tributarias de la entidad investigada mediante una matriz de conciliación formals.

9.4 Identificación de beneficiarios finales

Objetivo

La identificación del beneficiario final constituye la cuarta etapa de la metodología: determinar la persona natural que, directa o indirectamente, posee, controla o ejerce influencia significativa sobre los activos u operaciones investigadas, trascendiendo la titularidad aparente de billeteras, cuentas o VASP para establecer quién ejerce el control efectivo y obtiene el beneficio económico, como elemento esencial para atribuir responsabilidades y fortalecer el valor probatorio de la investigación.

Fundamento técnico

Uno de los principales desafíos de las investigaciones sobre criptoactivos consiste en diferenciar la identidad digital observada en la blockchain de la identidad real de las personas que controlan los activos virtuales. Aunque las redes blockchain registran de forma permanente todas las transacciones realizadas, estas generalmente se encuentran asociadas a direcciones criptográficas y no a identidades verificadas, lo que dificulta la atribución inmediata de las operaciones.

Por esta razón, la identificación del beneficiario final requiere integrar información procedente de diversas fuentes, como registros de conocimiento del cliente (KYC), información de proveedores de servicios de activos virtuales (VASP), documentación financiera, registros societarios, bases de datos públicas, inteligencia de fuentes abiertas (OSINT), análisis de redes financieras y herramientas especializadas de analítica blockchain.

Las Recomendaciones del Grupo de Acción Financiera Interamericana (FATF, 2023) establecen que la identificación del beneficiario final constituye un componente esencial del enfoque basado en riesgos para prevenir el lavado de activos y el financiamiento del terrorismo. Asimismo, los estándares interamericanos promueven la transparencia sobre la propiedad y el control efectivo de personas jurídicas y estructuras complejas, especialmente cuando intervienen activos virtuales y operaciones transfronterizas.

Desde la perspectiva de la auditoría forense, la identificación del beneficiario final debe sustentarse en evidencia suficiente, adecuada y verificable, evitando inferencias no respaldadas documentalmente. Las conclusiones alcanzadas deberán derivarse de la correlación objetiva entre la evidencia digital, financiera, documental y tecnológica recopilada durante la investigación.

Procedimientos

Durante esta etapa el auditor forense desarrollará, entre otros, los siguientes procedimientos:

- **Identificar los sujetos involucrados:** Personas naturales, personas jurídicas, proveedores de servicios de activos virtuales (VASP), exchanges centralizados, exchanges descentralizados, custodios de activos virtuales, fideicomisos y otras estructuras jurídicas, así como Organizaciones Autónomas Descentralizadas (DAO), cuando resulte pertinente.
- **Identificar las billeteras relacionadas:** Wallets de origen, receptoras, intermediarias, de autocustodia, institucionales y direcciones vinculadas mediante herramientas de clustering.
- **Obtener información de identificación:** Recopilar y analizar información KYC, información de Debida Diligencia, documentación societaria, registros mercantiles, registros tributarios, información bancaria, registros de proveedores de activos virtuales, información obtenida mediante requerimientos judiciales o administrativos, y fuentes abiertas (OSINT).
- **Correlacionar la información:** El auditor deberá relacionar direcciones blockchain, identidades verificadas, dispositivos utilizados, direcciones IP (cuando legalmente proceda), correos electrónicos, números telefónicos, registros de autenticación, información financiera tradicional y relaciones comerciales y societarias.

- **Analizar el control efectivo:** Determinar quién controla las claves privadas, autoriza las operaciones, decide el destino de los activos, obtiene el beneficio económico, controla sociedades vinculadas y administra plataformas o protocolos relacionados con las operaciones.
- **Validar la información obtenida:** Las conclusiones deberán contrastarse mediante múltiples fuentes independientes, procurando evitar atribuciones basadas exclusivamente en una única evidencia tecnológica o documental.

Matriz de atribución y grado de certeza

La identificación de una persona detrás de una dirección blockchain deberá expresarse conforme al nivel de corroboración alcanzado. La coincidencia técnica o el clustering de direcciones no equivalen, por sí solos, a una identificación jurídica del titular o beneficiario final.

A efectos metodológicos, podrá utilizarse la siguiente escala de atribución:

- **Nivel 1 - Asociación técnica:** Existencia de vínculos transaccionales, heurísticas de clustering u otras relaciones observables entre direcciones.
- **Nivel 2 - Asociación contextual:** Coincidencia de patrones temporales, contrapartes, dispositivos, datos de acceso, comunicaciones u otros elementos contextuales compatibles.
- **Nivel 3 - Asociación documental:** Existencia de información KYC, registros de proveedores de servicios, documentación bancaria, societaria, contractual o tributaria que vincula una identidad con la dirección o cuenta analizada.
- **Nivel 4 - Atribución corroborada:** Convergencia de múltiples fuentes independientes, técnicas y documentales, que permiten sostener razonablemente el control efectivo o beneficio económico.

El nivel asignado deberá constar en los papeles de trabajo y en el informe cuando sea relevante. El auditor evitará afirmaciones categóricas de titularidad cuando la evidencia solo permita hablar de asociación, vinculación probable o control inferido.

Herramientas recomendadas

Se emplean las plataformas de blockchain analytics y OSINT del Capítulo 10, más fuentes propias de esta etapa: registros públicos de sociedades, de beneficiarios finales, tributarios y judiciales.

Documentación obtenida

- Como resultado de esta etapa podrán recopilarse y elaborarse los siguientes documentos:
- Perfil del beneficiario final.
- Árbol de propiedad y control.
- Organigrama societario.
- Relación entre personas naturales y jurídicas.
- Registro de billeteras vinculadas.
- Reportes KYC.
- Documentación societaria.
- Informes de blockchain analytics.
- Registros de correlación entre identidades y direcciones blockchain.
- Informes de inteligencia financiera.
- Evidencia documental de control efectivo.

Toda la documentación deberá conservarse conforme a los procedimientos de cadena de custodia y a las normas aplicables sobre protección de datos y confidencialidad.

Riesgos frecuentes

- Durante la identificación del beneficiario final pueden presentarse, entre otros, los siguientes riesgos:
- Confundir al titular registrado con el verdadero controlador de los activos.
- Basar las conclusiones exclusivamente en información blockchain.
- No considerar estructuras societarias multinivel.
- Omitir el análisis de testaferros o intermediarios.
- No identificar relaciones familiares o empresariales relevantes.
- Dependencia excesiva de bases de datos comerciales.
- Información KYC desactualizada o insuficiente.
- Uso de documentación falsificada.
- Intervención de jurisdicciones con baja transparencia.
- Utilización de mecanismos tecnológicos destinados a ocultar la identidad.
- Atribución indebida de billeteras mediante análisis insuficiente.
- Vulneración de normas sobre privacidad o protección de datos durante la obtención de información.

Papeles de trabajo

Como evidencia del trabajo desarrollado deberán prepararse, entre otros, los siguientes papeles de trabajo:

- Cédula de identificación del beneficiario final.
- Matriz de propiedad y control.
- Hoja de análisis societario.
- Registro de billeteras vinculadas.
- Cédula de correlación de identidades.
- Hoja de verificación KYC.
- Matriz de relaciones entre personas y entidades.
- Diagrama de estructuras societarias.
- Registro de validación de información.
- Referencias cruzadas con el perfil transaccional y la matriz de riesgos.

Cada papel de trabajo deberá indicar las fuentes consultadas, la evidencia utilizada, los procedimientos aplicados y el grado de confiabilidad de la información analizada.

Producto esperado

Al concluir esta etapa, el auditor forense debe contar con una identificación técnicamente sustentada del beneficiario final —respaldada por evidencia documental, financiera y digital que demuestre el control efectivo o beneficio económico, y no solo la titularidad formal, estableciendo los vínculos entre personas, entidades y estructuras societarias necesarios para la reconstrucción de redes y el informe pericial.

9.5 Técnicas de Visualización de Redes Financieras

Objetivo

La visualización de redes financieras constituye la quinta etapa de la metodología: representar gráficamente las relaciones entre personas, billeteras, VASP, plataformas de intercambio, contratos inteligentes y demás actores, para identificar nodos relevantes, patrones de interacción, flujos de activos y posibles mecanismos de ocultamiento, transformando grandes volúmenes de datos en información visual que facilite el análisis y la comunicación de los hallazgos.

Fundamento técnico

Las investigaciones sobre criptoactivos generan grandes cantidades de datos estructurados y no estructurados, cuya interpretación resulta compleja cuando se analizan únicamente mediante tablas o registros cronológicos. En este contexto, las técnicas de visualización de redes financieras constituyen una herramienta analítica que permite representar gráficamente las relaciones entre los distintos elementos de la investigación, facilitando la identificación de

estructuras organizadas, intermediarios, concentraciones de activos, patrones de comportamiento y vínculos financieros que podrían pasar inadvertidos mediante un análisis convencional.

Desde la perspectiva del análisis de redes (Network Analysis), cada dirección blockchain, persona, entidad, contrato inteligente o proveedor de servicios puede representarse como un nodo, mientras que las transacciones, relaciones societarias o vínculos económicos constituyen las conexiones o aristas entre dichos nodos. Este enfoque permite comprender la estructura global de una red financiera y detectar elementos relevantes como nodos centrales, intermediarios, comunidades, rutas predominantes de circulación de activos y posibles mecanismos de dispersión o concentración de recursos.

Asimismo, la utilización de herramientas de visualización fortalece la calidad del informe pericial al facilitar la explicación técnica de operaciones complejas ante autoridades administrativas, fiscales o judiciales. No obstante, la representación gráfica constituye un medio de análisis y comunicación, por lo que las conclusiones siempre deberán sustentarse en evidencia objetiva, suficiente y verificable, conforme a los principios establecidos por las Normas Interamericanas de Auditoría (IAASB, 2022).

Procedimientos

Durante esta etapa el auditor forense desarrollará, entre otros, los siguientes procedimientos:

- **Consolidar la información relacional:** Integrar la información obtenida durante las etapas anteriores, incluyendo personas naturales y jurídicas, direcciones blockchain, billeteras digitales, exchanges, proveedores de servicios de activos virtuales (VASP), contratos inteligentes, protocolos DeFi, cuentas bancarias relacionadas y beneficiarios finales identificados.
- **Definir los elementos de la red:** El auditor deberá establecer nodos (personas, empresas, wallets, exchanges, contratos inteligentes, tokens, plataformas DeFi y DAO) y conexiones (transferencias de activos virtuales, relaciones societarias, control accionario, beneficiarios finales, contratos comerciales, interacción con protocolos blockchain y relaciones económicas verificadas).
- **Construir la red financiera:** Una vez identificados los nodos y sus relaciones, deberá elaborarse la representación gráfica de la estructura financiera considerando dirección del flujo de activos, valor económico, frecuencia de interacción, temporalidad, intensidad y nivel de riesgo de cada nodo.

- **Analizar la estructura de la red:** Identificar nodos con alta concentración de operaciones, intermediarios relevantes, centros de control, comunidades financieras, redes altamente conectadas, billeteras puente, patrones repetitivos y rutas de dispersión o concentración de activos. Evaluar indicadores como centralidad, intermediación (betweenness), cercanía (closeness), densidad de la red, grado de conectividad y componentes aislados.
- **Identificar estructuras complejas:** Analizar la existencia de redes de lavado de activos, estructuras de testaferros, empresas pantalla, billeteras controladas por un mismo beneficiario, operaciones circulares, redes multinivel, mezcladores (mixers), puentes entre blockchains (cross-chain bridges) y protocolos de anonimización.
- **Documentar las visualizaciones:** Cada representación gráfica deberá contener fecha de elaboración, fuente de información, herramienta utilizada, criterios de construcción, descripción de símbolos, leyenda de nodos y conexiones, e interpretación técnica. Se incorporarán como evidencia complementaria y no sustituirán el análisis documental.

Continuidad económica del valor en redes complejas

En la visualización de redes multicadena se deberá procurarse representar no solo la continuidad técnica de una dirección o token, sino también la continuidad económica del valor. Un mismo flujo puede transformarse sucesivamente mediante swaps, wrapped tokens, bridges, pools de liquidez o contratos inteligentes sin que exista una ruptura económica de la operación investigada.

Las visualizaciones deberán distinguir con simbología específica los cambios de red, transformaciones de activos, operaciones internas de protocolos y puntos de entrada o salida hacia proveedores custodios o sistema financiero tradicional, reduciendo el riesgo de doble conteo.

Herramientas recomendadas

Se emplean las plataformas de blockchain analytics y visualización de redes del Capítulo 10, más herramientas generales de inteligencia financiera y bases de datos orientadas a grafos.

Documentación obtenida

Diagramas de redes financieras, mapas de relaciones, grafos de transacciones blockchain, diagramas de flujo de activos, árboles de control societario, mapas de beneficiarios finales, reportes de centralidad, reportes de comunidades, cronologías visuales e informes gráficos de reconstrucción financiera.

Riesgos frecuentes

Incorporar relaciones no sustentadas en evidencia, confundir correlación con causalidad, interpretar incorrectamente la dirección de los flujos, excluir nodos relevantes, saturar los diagramas, no actualizar la red, basar las conclusiones exclusivamente en el gráfico u omitir relaciones indirectas.

Papeles de trabajo

Cédula de construcción de la red financiera, matriz de nodos identificados, registro de conexiones verificadas, hoja de análisis de centralidad, cédula de análisis de comunidades, inventario de visualizaciones, registro de versiones y hoja de validación de relaciones.

Producto esperado

Una representación gráfica integral, reproducible y verificable de la red financiera investigada, que permita identificar estructuras complejas, rutas de circulación de activos, nodos estratégicos y beneficiarios finales.

9.6 Evidencia Pericial en Procesos Judiciales

Objetivo

La obtención y presentación de la evidencia pericial constituye la sexta etapa de la metodología: recopilar, preservar, analizar, documentar y presentar evidencia digital de operaciones con criptoactivos garantizando su autenticidad, integridad, trazabilidad, confiabilidad y admisibilidad, de modo que las conclusiones de la investigación puedan sustentarse técnicamente conforme al debido proceso, la cadena de custodia y las normas interamericanas de auditoría e investigación forense.

Fundamento técnico

La evidencia constituye el elemento central de toda investigación forense. En el ámbito de los criptoactivos, la evidencia adquiere una dimensión particularmente compleja debido a que gran parte de la información relevante se encuentra almacenada en entornos digitales distribuidos, plataformas tecnológicas, dispositivos electrónicos y registros criptográficos generados por redes blockchain.

Aunque las transacciones registradas en blockchain poseen características de inmutabilidad y verificabilidad criptográfica, ello no implica que, por sí mismas, constituyan prueba suficiente para atribuir responsabilidades jurídicas. La labor del auditor forense consiste en integrar la evidencia blockchain con

documentación financiera, registros contables, información de proveedores de servicios de activos virtuales (VASP), registros KYC, información bancaria, evidencia informática y demás elementos probatorios.

Procedimientos

- **Identificar la evidencia relevante:** Registros blockchain, hashes de transacciones, direcciones de billeteras, contratos inteligentes, reportes de blockchain analytics, registros de exchanges, KYC, registros bancarios, estados financieros, dispositivos electrónicos, correos electrónicos y registros de autenticación.
- **Obtener la evidencia:** Garantizar legalidad, integridad, autenticidad de la fuente, registro cronológico de actuaciones, identificación del responsable y preservación del formato original.
- **Preservar la evidencia digital:** Cálculo de valores hash, generación de imágenes forenses, copias maestras y de trabajo, protección contra modificaciones, almacenamiento seguro y registro continuo de la cadena de custodia.
- **Validar la evidencia:** Confirmación de autenticidad, verificación de consistencia, contraste con fuentes independientes, correlación financiera-blockchain, confirmación cronológica de eventos y revisión técnica.
- **Clasificar la evidencia:** Documental, digital, financiera y tecnológica.
- **Documentar la evidencia:** Código de identificación, descripción, fecha/hora, fuente, responsable, método, valor hash, ubicación, referencia de cadena de custodia y relación con los hechos.

Validación de herramientas de blockchain analytics y principio de no dependencia algorítmica

Las plataformas de blockchain analytics constituyen herramientas auxiliares para organizar, enriquecer y visualizar información, pero sus etiquetas, agrupamientos, puntuaciones de riesgo o inferencias no deberán considerarse evidencia concluyente de manera automática. El auditor conserva la responsabilidad profesional sobre la interpretación de los resultados.

Cuando una conclusión relevante dependa de una herramienta automatizada, deberá documentarse el nombre y versión de la plataforma, fecha y hora del análisis, redes y activos analizados, parámetros y filtros utilizados, etiquetas o heurísticas de clustering aplicadas, fuente de las etiquetas, limitaciones técnicas (falsos positivos/negativos) y el procedimiento de contraste con exploradores blockchain o registros primarios.

La inteligencia artificial y los modelos de aprendizaje automático podrán emplearse como mecanismos auxiliares, pero sus resultados deberán ser ex-

plicables, verificables y sometidos a juicio profesional, sin sustituir la evidencia primaria ni la conclusión del perito.

Herramientas recomendadas

Plataformas de blockchain analytics e informática forense del Capítulo 10, más herramientas generales de gestión documental y de expedientes.

Documentación obtenida y Riesgos frecuentes

Inventario de evidencia, actas de obtención, formularios de cadena de custodia, registros de valores hash, reportes blockchain analytics e informes de informática forense. *Riesgos:* Ruptura de la cadena de custodia, alteración involuntaria de archivos, obtención sin autorización legal, pérdida de metadatos, contaminación de evidencia o dependencia de una única fuente.

Papeles de trabajo y Producto esperado

Programas de obtención, inventario de evidencia digital, actas de cadena de custodia, registros de cálculo HASH y hojas de validación. *Producto:* Expediente pericial estructurado, organizado, clasificado, preservado y verificable de forma independiente.

9.7 Elaboración de Informes Técnicos

Objetivo

La elaboración del informe técnico constituye la etapa final de la metodología: documentar de manera clara, objetiva y técnicamente fundamentada los procedimientos, la evidencia, los análisis y las conclusiones de la investigación, como principal medio de comunicación entre el auditor forense y las autoridades administrativas, judiciales o fiscales, sin emitir juicios jurídicos sobre responsabilidad, sino presentando los resultados periciales para que la autoridad competente valore la evidencia conforme a las normas procesales aplicables.

Fundamento técnico

El informe técnico sintetiza todo el proceso de investigación financiera digital. Su elaboración debe observar los principios de independencia, objetividad, competencia profesional, debido cuidado, integridad y confidencialidad, garantizando que las conclusiones deriven exclusivamente de la evidencia obtenida. Las Normas Interamericanas de Auditoría (IAASB, 2022) exigen que las conclusiones estén respaldadas por evidencia suficiente y adecuada.

Procedimientos

- **Revisar el expediente de investigación:** Verificar integridad, suficiencia de evidencia, cadena de custodia y consistencia entre papeles de trabajo y conclusiones.
- **Organizar la información:** Clasificar conforme a antecedentes, objetivos, alcance, metodología, evidencia obtenida, hallazgos, análisis, conclusiones y anexos.
- **Redactar los hallazgos:** Descripción del hecho, evidencia de respaldo, procedimiento aplicado, riesgo identificado, impacto observado y referencias a papeles de trabajo.
- **Elaborar las conclusiones:** Objetivas, verificables, derivadas directamente de la evidencia, sin opiniones jurídicas y coherentes con los hallazgos.
- **Formular recomendaciones:** Fortalecimiento del control interno, gestión de riesgos, cumplimiento normativo, conservación de evidencia y medidas preventivas.
- **Revisar el informe:** Verificación de consistencia técnica, corrección metodológica, exactitud de cifras, referencias documentales y calidad de redacción.

Riesgos frecuentes

Emitir conclusiones no sustentadas, incorporar opiniones jurídicas, omitir limitaciones, redacción ambigua, inconsistencias entre hallazgos y conclusiones, falta de referencias a la evidencia, uso de jerga sin explicar o divulgación de información confidencial.

Ejemplo Estándar de Informe Técnico Pericial

INFORME TÉCNICO DE INVESTIGACIÓN FINANCIERA DIGITAL

Número de Informe: ITFD-001/2026

Entidad solicitante: _____

Autoridad requirente: _____

Auditor Forense: _____

Fecha: _____

I. Antecedentes

Descripción del requerimiento recibido, hechos investigados y contexto general del caso.

II. Objeto de la investigación

Precisar el propósito del trabajo pericial, indicando las operaciones, personas, billeteras digitales o activos virtuales objeto de análisis.

III. Alcance

Período analizado.

Redes blockchain examinadas.

Exchanges involucrados.

Documentación revisada.

Limitaciones encontradas.

Grado de certeza de las atribuciones y limitaciones de las herramientas analíticas utilizadas.

IV. Metodología aplicada

Descripción de la metodología utilizada, incluyendo recolección de información financiera digital, evaluación de riesgos, perfilamiento transaccional, identificación del beneficiario final, reconstrucción de redes financieras y validación de evidencia digital.

V. Análisis de los hechos y hallazgos periciales

Exposición sistemática y cronológica de los hallazgos obtenidos mediante el cruce de la evidencia *on-chain*, los registros contables y la documentación financiera, detallando la descripción de la anomalía, la evidencia técnica de respaldo (hashes, identificadores) y la valoración económica y patrimonial.

VI. Conclusiones periciales

Síntesis lógica y objetiva derivada estrictamente de la evidencia analizada, respondiendo a los objetivos planteados en la investigación sin emitir juicios de valor jurídico sobre la culpabilidad penal o civil.

VII. Recomendaciones técnicas

Sugerencias orientadas a la mitigación de riesgos, fortalecimiento del control interno, revisión de políticas de debida diligencia o preservación de la evidencia digital.

VIII. Anexos

Anexo No. 1: Matriz detallada de transacciones y rastreo *on-chain*.

Anexo No. 2: Diagramas de redes financieras y grafos de correlación de nodos.

Anexo No. 3: Inventario de la cadena de custodia digital y valores hash (SHA-256)

PARTE IV

Herramientas, Analítica y Tecnología Forense

10 HERRAMIENTAS ESPECIALIZADAS DE ANÁLISIS BLOCKCHAIN

10.1 Plataformas Blockchain

La tecnología blockchain ha evolucionado desde su utilización inicial con Bitcoin hacia infraestructuras capaces de soportar contratos inteligentes, aplicaciones descentralizadas, trazabilidad, tokenización, pagos y soluciones empresariales. En auditoría forense puede proporcionar registros cronológicos, verificables y resistentes a alteraciones; sin embargo, su valor probatorio depende del diseño de la red, la calidad de los datos de origen y los procedimientos de auditoría aplicados.

10.1.1 Principales plataformas

Ethereum: Red pública orientada a smart contracts y aplicaciones descentralizadas. Permite analizar transacciones, direcciones, tokens, eventos y contratos inteligentes.

Hyperledger Fabric: Plataforma empresarial permissioned con identidades, permisos y controles de acceso. Es especialmente útil para trazabilidad, control interno e intercambio de información.

Solana: Blockchain pública de alto rendimiento, útil para análisis de grandes volúmenes de operaciones y patrones de actividad automatizada.

Polygon: Infraestructura vinculada al ecosistema Ethereum, orientada a escalabilidad, pagos, activos digitales y aplicaciones empresariales.

Bitcoin: Red pública cuyo historial transaccional puede analizarse mediante direcciones, movimientos, fechas y montos.

Corda: Plataforma orientada a transacciones entre organizaciones, con especial interés en los sectores empresarial y financiero.

10.1.2 Tabla comparativa de plataformas

Aspecto	Ethereum	Fabric	Solana	Polygon	Bitcoin
Red pública	Sí	No	Sí	Sí	Sí
Acceso autorizado	No	Sí	No	No	No
Smart contracts	Sí	Sí	Sí	Sí	Limitado
Uso empresarial	Alto	Muy alto	Alto	Alto	Medio
Trazabilidad	Alta	Muy alta	Alta	Alta	Muy alta
Auditoría forense	Muy alta	Muy alta	Alta	Alta	Muy alta

10.1.3 Aplicación en auditoría forense

Trazabilidad de transacciones.
Análisis de direcciones y movimientos.
Auditoría de smart contracts.
Identificación de patrones y relaciones.
Documentación de transacciones como evidencia digital.

10.1.4 Consideración para Ecuador

Debe distinguirse la tecnología blockchain de los criptoactivos. El Banco Central del Ecuador ha señalado que los criptoactivos no son moneda de curso legal ni medios de pago autorizados en Ecuador. Esto no elimina el interés tecnológico de blockchain para procesos empresariales, pero exige analizar separadamente el tratamiento jurídico, contable y tributario de cada operación.

10.2 Herramientas OSINT aplicadas a la Auditoría Forense

OSINT (Open Source Intelligence) comprende la obtención, análisis y correlación de información disponible legalmente en fuentes abiertas. En auditoría forense permite generar y corroborar indicios sobre personas, empresas, dominios, relaciones y hechos.

Herramientas y fuentes

- **Google y Bing:** Búsquedas avanzadas de información pública.

- **Google Lens:** Búsqueda y verificación de imágenes.
- **Wayback Machine:** Consulta de versiones históricas de sitios web.
- **WHOIS/RDAP:** Información pública sobre dominios.
- **Maltego:** Correlación de personas, empresas, dominios y otras entidades.
- **SpiderFoot:** Automatización de reconocimiento y correlación OSINT.
- **Shodan:** Identificación de activos tecnológicos expuestos públicamente.
- **VirusTotal:** Análisis de indicadores técnicos.
- **Registros públicos y redes profesionales:** Corroboración de información empresarial.

Metodología OSINT

Definir el objetivo identificar entidades recopilar información correlacionar verificar mediante fuentes independientes preservar documentar formular conclusiones.

Principio de legalidad

OSINT no equivale a hacking. La investigación debe limitarse a información legalmente accesible y respetar las normas aplicables de privacidad, protección de datos y acceso a información.

10.3 Exploradores Blockchain

Los exploradores blockchain permiten consultar información registrada en determinadas redes, incluyendo direcciones, transacciones, bloques, fechas, montos, comisiones, tokens y contratos.

Principales exploradores

- **Etherscan** – Ethereum y redes EVM.
- **Blockchair** – Análisis de multiples blockchains.
- **Solscan** – Solana.
- **Mempool.space** – Bitcoin.
- **Blockchain.com Explorer** – Bitcoin y otras redes.
- **BscScan** – BNB Smart Chain.
- **Arbiscan** – Arbitrum.
- **Basescan** – Base.
- **Procedimiento forense**

Dirección o identificador explorador transacciones fechas y montos contrapartes correlación con documentos contables preservación de la referencia conclusión.

La identificación de una dirección blockchain no demuestra por sí sola quién es su propietario. Debe corroborarse mediante otras fuentes y evidencia independiente.

10.4 Inteligencia Artificial aplicada al Análisis Financiero

La Inteligencia Artificial aplicada al análisis financiero utiliza algoritmos para procesar grandes volúmenes de información, identificar patrones, detectar anomalías y apoyar la evaluación de riesgos.

Aplicaciones

- Detección de transacciones anómalas.
- Identificación de facturas duplicadas.
- Detección de proveedores con comportamiento atípico.
- Análisis de partes relacionadas.
- Predicción de tendencias y flujo de caja.
- Clasificación y análisis de documentos.

IA y auditoría forense

Datos financieros limpieza IA/analítica anomalías investigación OSINT corroboración documental evidencia conclusión del auditor.

Riesgos

Datos incompletos o incorrectos, falsos positivos y falsos negativos, sesgos algorítmicos, falta de explicabilidad, riesgos de confidencialidad y dependencia excesiva de resultados automatizados. *La IA genera análisis y alertas; el auditor verifica, interpreta y documenta la evidencia.*

10.5 Automatización y Analítica Avanzada

La automatización permite ejecutar tareas repetitivas de manera sistemática. La analítica avanzada utiliza estadística, minería de datos, aprendizaje automático y otras técnicas para descubrir patrones y anomalías.

Aplicaciones y Técnicas

- **Aplicaciones:** Detección automatizada de facturas duplicadas, identificación de pagos fuera de horario, detección de operaciones fraccionadas, análisis de concentración de proveedores e identificación de cambios anormales en ingresos y gastos.
- **Técnicas:** Data Analytics, detección de anomalías, clustering, regresión, Machine Learning, Process Mining, Link Analysis, Text Mining y visualización de datos.

Process Mining

Permite reconstruir procesos a partir de registros digitales. Por ejemplo, puede revelar que una misma persona solicita, aprueba y autoriza pagos cuando las políticas internas exigen segregación de funciones.

10.6 Gestión de la Evidencia Digital

La evidencia digital comprende información electrónica que puede contribuir a demostrar, confirmar o refutar hechos relevantes para una investigación.

- **Fuentes:** Sistemas contables y ERP, correos electrónicos, computadoras y dispositivos móviles, bases de datos y registros de acceso, redes sociales, sitios web, blockchain, plataformas de pago y documentos electrónicos.
- **Ciclo de gestión:** Identificación adquisición preservación documentación análisisvalidación presentación custodia.
- **Cadena de custodia y Hash:** Debe registrarse quién tuvo acceso a la evidencia, qué recibió, cuándo y mediante qué método. Una función hash (como SHA-256) genera una huella digital inalterable del archivo.

10.7 Integración de Tecnologías en la Auditoría Forense

La integración de las tecnologías anteriores permite ampliar la capacidad del auditor para analizar grandes volúmenes de información, descubrir relaciones y preservar evidencia digital.

Modelo integrado

Información financiera automatización IA y analítica anomalías OSINT Blockchain/Exploradores corroboración documental preservación de evidencia análisis forense informe.

Caso práctico integrado

Una empresa comercial presenta 5.000 pagos a proveedores. La analítica identifica 18 operaciones atípicas, cinco proveedores con datos de contacto similares, tres pagos fuera del horario habitual, dos facturas con características coincidentes y un proveedor constituido recientemente. La IA y la analítica priorizan las operaciones. OSINT identifica coincidencias públicas entre proveedores. Un pago relacionado con un activo digital se verifica mediante un explorador blockchain. Cada elemento se preserva y documenta como evidencia. El auditor correlaciona proveedor, cuenta bancaria, aprobadores, documentos y transacciones.

Regla de conclusión

Indicio corroboración evidencia análisis profesional conclusión. Una alerta tecnológica o una coincidencia OSINT no demuestra por sí sola la existencia de fraude.

11 ANÁLISIS FORENSE DE OPERACIONES CRIPTO

11.1 Identificación de patrones sospechosos

Para identificar patrones sospechosos, trazar fondos o reconstruir flujos de activos digitales dentro de un proceso investigativo, es necesario dominar los aspectos fundamentales que permiten comprender cómo se registra cada operación en la blockchain y en las redes compatibles. Para cualquier análisis forense riguroso, las cadenas de bloques dejan huellas distintivas que permiten la trazabilidad.

Al registrarse una transacción en la blockchain de Ethereum y en redes similares, resulta indispensable comprender que ETH no es simplemente un libro de movimientos de dinero, sino una computadora global, descentralizada y pública, en la que se ejecutan transacciones tan simples como el envío de ether entre personas, o tan complejas como la ejecución de una serie de instrucciones automáticas definidas en contratos inteligentes que interactúan entre sí dentro de la cadena.

Protagonistas de una transacción en la blockchain de Ethereum

- **Cuenta de Propiedad Externa (EOA, Externally Owned Account):** Es una cuenta controlada por una persona a través de una clave privada; cualquier billetera de usuario es una EOA. Una EOA puede enviar ETH, iniciar transacciones y firmar mensajes. Lo que no puede hacer es ejecutar código por sí sola.
- **Contrato inteligente (Smart Contract):** Es una cuenta que contiene código programado. No tiene un propietario en el tradicional: se ejecuta automáticamente cuando alguien lo invoca. La regla fundamental es que toda transacción en Ethereum es iniciada siempre por una EOA, nunca por un contrato.

Arquitectura de una transacción

- **Transaction Hash:** Identificador único de la transacción obtenido aplicando Keccak-256 (SHA-3). Es el equivalente al número de expediente de un caso.
- **Status:** Indica si la transacción fue procesada con éxito ("Success") o si falló ("Failed"). Una transacción fallida también queda registrada y consume gas.
- **Block y Timestamp:** Número de bloque y fecha/hora exacta en UTC en que el bloque fue validado.
- **From:** Dirección EOA que originó la transacción (quien firma es quien paga).
- **To / Interacted With:** Dirección de destino o contrato inteligente invocado.
- **Value:** Monto de ETH nativo transferido (puede ser 0 en transferencias de tokens ERC-20).
- **ERC-20 Tokens Transferred:** Campo que registra la transferencia de tokens (USDC, USDT, DAI) mediante eventos *Transfer*.
- **Transaction Fee:** Costo total pagado por incluir la transacción (Gas Used $\times$ Gas Price).

Mecanismo EIP-1559

Implementado el 5 de agosto de 2021, transformó el sistema de cobro de comisiones:

- **Tarifa base (Base Fee):** Costo automático según la congestión de la red.
- **Quema (Burning):** La tarifa base se elimina permanentemente de la circulación.
- **Propina (Tip):** Pago adicional opcional al validador para priorizar la transacción.
- **Gas Price:** Expresado en gwei (1gwei = 0.000000001 ETH).
- **Input Data:** Datos enviados al contrato (código ABI) o vacío ("0x") en transferencias simples.

Tabla No. 5

Comparación entre transacción nativa y transacción de contrato en Ethereum

Característica	Transacción nativa	Transacción de contrato
Input Data	Vacío ("0x"); sin código que ejecutar.	Contiene datos codificados (ABI encoding) con funciones y parámetros.

Característica	Transacción nativa	Transacción de contrato
Gas usado	Exactamente 21.000 unidades (estándar).	Variable y superior, según el costo computacional del código.
Value	Monto transferido expresado en ETH.	Puede ser 0 ETH si el valor se mueve como token.
Logs / eventos	No hay logs ni eventos.	Aparecen logs con los eventos emitidos por el contrato.
Transacciones internas	No existen.	Pueden aparecer llamadas que el contrato hace a otros contratos (subtransacciones EVM).
Tokens ERC-20	No aparece este campo.	Puede aparecer si involucra tokens ERC-20.
Complejidad forense	Muy baja: flujo directo.	Mayor: requiere revisar logs, parámetros decodificados y transacciones internas.

11.2 Tipologías de ocultamiento financiero

Las organizaciones criminales han adaptado las técnicas tradicionales de lavado al ecosistema digital:

Tabla No. 6

Tipologías de ocultamiento financiero en activos digitales

Tipología	Mecanismo operativo	Indicador de riesgo (red flag)
Estructuración digital (smurfing)	División de grandes sumas en múltiples depósitos pequeños por debajo de los límites de reporte de los PSAV.	Múltiples cuentas con patrones de identidad similares que reciben fondos coordinados en poco tiempo.
Arbitraje regulatorio internacional	Movilización rápida de activos hacia jurisdicciones de baja regulación o sin riguroso KYC.	Retiros inmediatos hacia direcciones externas tras recibir fondos de exchanges institucionales.
Facturación simulada mediante NFT	Uso de contratos inteligentes en marketplaces para comprar y vender colecciones propias a precios inflados (wash trading).	Intercambio de NFT de baja liquidez entre direcciones vinculadas a un mismo origen.

Señales de alerta (*Red Flags*) operativas y de anonimato

Estructurar operaciones por debajo de los umbrales obligatorios de reporte.

Realizar múltiples operaciones de alto valor en 24 horas o patrones escalonados típicos de *ransomware*.

Transferencias inmediatas a múltiples PSAV en jurisdicciones con regulaciones débiles o ausentes.

Uso de mezcladores (*mixers*), monedas de privacidad (*Monero*, *Zcash*), servicios P2P no regulados o pasarelas de anonimización (VPN, red oscura).

Irregularidades en debida diligencia y perfiles: Información KYC incompleta, uso de documentos falsificados o editados, clientes inusualmente mayores operando grandes volúmenes, o personas en situación de vulnerabilidad financiera utilizadas como **mulas de dinero**, perfil caracterizado por la cesión de cuentas o la realización de operaciones fraccionadas para el blanqueo

11.3 Casos de layering digital

El término layering proviene del inglés layer, que significa «capa». El objetivo de esta fase no es ocultar la existencia de los activos digitales, sino superponer tantas capas de transacciones consecutivas como sea posible para dificultar su rastreo.

Es importante no confundir este concepto con layer 1, layer 2 y layer 3, términos que se refieren a las capas de infraestructura y escalabilidad de una red blockchain.

La fase de estratificación, o layering, busca distanciar los fondos de su fuente ilícita mediante una red compleja de transacciones financieras. En el ámbito cripto, el layering digital se ejecuta de forma casi instantánea a través de arquitecturas automatizadas:

Dispersión multicapa: los fondos se retiran de un mercado ilícito y se dividen entre veinte y cincuenta billeteras distintas, controladas por software automatizado.

Conversión de cripto a cripto (token swapping): utilización de plataformas de intercambio descentralizadas (DEX) para convertir los criptoactivos originales —por ejemplo, BTC o ETH— en stablecoins como USDT o USDC, lo que rompe el hilo conductor directo del libro contable cuando los investigadores monitorean un único estándar de token.

Pasarelas de liquidación automatizadas: envío de los fondos a procesadores de pago comerciales independientes que convierten los criptoactivos en tarjetas de regalo, créditos de videojuegos o bienes digitales de alta liquidez, antes de reingresarlos al sistema financiero tradicional.

11.4 Cross-chain transactions

El fenómeno conocido como chain-hopping constituye uno de los desafíos más complejos para la atribución forense. Consiste en mover fondos entre diferentes cadenas de bloques independientes —por ejemplo, saltar de la red de Bitcoin a Ethereum, y luego a Solana o a Binance Smart Chain— con el fin específico de romper el rastreo lineal de las herramientas analíticas estándar.

Los principales vectores técnicos que facilitan el ocultamiento intercadena son los siguientes:

- **Puentes descentralizados (cross-chain bridges).** Protocolos basados en contratos inteligentes de tipo «bloquear y emitir» (lock-and-mint) o en pools de liquidez intercadena. El usuario deposita un activo en la Cadena A y recibe un activo sintético o equivalente en la Cadena B. El análisis forense requiere mapear, de manera simultánea, los eventos emitidos por el contrato inteligente del puente en ambas redes, con el fin de correlacionar montos y marcas de tiempo.
- **Intercambiadores instantáneos sin registro (instant swappers).** Plataformas que no requieren la apertura de una cuenta de usuario y permiten intercambiar activos de diferentes redes mediante depósitos hacia direcciones temporales generadas dinámicamente, actuando como intermediarios opacos.

Características clave de la tecnología de cadena cruzada

Tabla No. 7

Características de la tecnología de interoperabilidad entre cadenas de bloques

N.º	Característica	Descripción
1	Interoperabilidad	Permite que las cadenas de bloques con diferentes protocolos y estructuras interactúen y compartan datos entre sí.
2	Transferencias de activos	Facilita el movimiento de tokens, NFT y otros activos entre cadenas de bloques sin intermediarios centralizados.
3	Descentralización	Los puentes y protocolos entre cadenas buscan mantener la ética descentralizada propia de la tecnología blockchain.
4	Utilidad mejorada	Los usuarios y desarrolladores pueden acceder a funciones y activos de múltiples cadenas de bloques, lo que habilita casos de uso innovadores.

Funcionamiento de la técnica de encadenamiento cruzado

Tabla No. 8

Mecanismos técnicos utilizados en las transacciones intercadena

N.º	Mecanismo	Descripción
1	Puentes de cadena cruzada	Protocolos que conectan dos o más cadenas de bloques, permitiendo la transferencia de activos e información entre ellas. Por ejemplo, Wormhole conecta Ethereum, Solana y otras redes.
2	Fichas envueltas (wrapped tokens)	Activos como Wrapped Bitcoin (WBTC) se emiten en una cadena de bloques para representar tokens de otra, manteniendo una paridad de uno a uno.
3	Protocolos de interoperabilidad	Protocolos como Polkadot y Cosmos proporcionan marcos para la comunicación entre cadenas y el intercambio de activos.
4	Intercambios atómicos	Los contratos inteligentes permiten intercambios directos de tokens entre pares a través de diferentes blockchains, sin necesidad de una plataforma de intercambio centralizada.

11.5 Privacy coins y anonimización

A diferencia de las redes pseudónimas como Bitcoin, en las que el registro de saldos y transacciones es completamente público, las monedas de privacidad implementan criptografía avanzada a nivel de protocolo para ocultar, de extremo a extremo, al emisor, al receptor y el monto transferido.

Conocidas también como monedas con anonimato mejorado (AEC, por sus siglas en inglés, Anonymity-Enhanced Cryptocurrencies), algunos ejemplos de monedas de privacidad son los siguientes:

- **Monero (XMR):** utiliza firmas de anillo y direcciones ocultas para disimular los detalles de las transacciones.
- **Zcash (ZEC):** emplea pruebas de conocimiento cero para permitir transacciones privadas.
- **Dash (DASH):** ofrece una función de privacidad opcional denominada PrivateSend.
- **MimbleWimble Extension Blocks (MWEB):** una función de privacidad implementada en la cadena de bloques de Litecoin, que permite a los usuarios optar por realizar transacciones que preserven su privacidad.

Criptografía en Monero (XMR)

Monero utiliza tres tecnologías criptográficas principales que impiden el análisis on-chain convencional:

- **Firmas de anillo (ring signatures).** Mezclan la firma del emisor real con firmas de transacciones pasadas extraídas de la blockchain. Esto hace que resulte, matemáticamente, imposible determinar cuál de las claves del grupo autorizó realmente el movimiento de fondos.
- **Direcciones ocultas (stealth addresses).** Obligan al emisor a crear, en nombre del receptor, una dirección pública única de un solo uso (one-time address) para cada transacción. Como resultado, no existe un historial público de transacciones vinculadas a una dirección de Monero fija en la red.
- **Transacciones confidenciales de anillo (RingCT).** Ocultan el valor real de la transacción mediante compromisos de Pedersen, lo que permite demostrar criptográficamente que la suma de las entradas es igual a la suma de las salidas, sin revelar los valores absolutos.

Criptografía en Zcash

Direcciones. Zcash cuenta con dos tipos de direcciones: privadas (direcciones z) y transparentes (direcciones t). Las direcciones z comienzan con la letra «z» y las direcciones t con la letra «t»; ambos tipos son interoperables, y los fondos pueden transferirse entre ellas. La protección o divulgación de información durante estas transacciones tiene implicaciones directas para la privacidad. Actualmente, la mayoría de las billeteras y plataformas de intercambio solo admiten direcciones t, aunque algunas billeteras móviles y de escritorio también admiten direcciones protegidas.

Transacciones. Las transacciones entre dos direcciones transparentes (t) funcionan igual que en Bitcoin: el remitente, el receptor y el valor de la transacción son visibles públicamente. Las transacciones que involucran direcciones protegidas incluyen las totalmente protegidas (z-to-z), las que blindan fondos (t-to-z) y las que los desblindan (z-to-t). La transacción más segura es la protegida (z-to-z), que cifra las direcciones del remitente y del receptor, así como el monto transferido. No obstante, todas las transacciones aparecen en la cadena de bloques pública, por lo que se sabe que una transacción se realizó y qué comisiones se pagaron.

Criptografía en Dash (DASH)

InstantSend. Permite a los usuarios transferir DASH sin esperar a que las transacciones se confirmen en la blockchain de Dash. En su lugar, los fondos se envían a nodos especiales, llamados «masternodos», que los bloquean antes de registrarlos en el siguiente bloque.

PrivateSend. Otra función de Dash, permite a los usuarios enviar transacciones mediante un servicio de mezcla integrado: los fondos se envían a masternodos, donde se combinan con los de otras transacciones, ocultando así el rastro de la operación original.

Criptografía en MimbleWimble Extension Blocks (MWEB)

Transacciones confidenciales (confidential transactions). Ocultan los montos enviados mediante el uso de compromisos de Pedersen (Pedersen commitments), lo que permite sumar los valores de entrada y salida para comprobar que coinciden, sin revelar públicamente las cantidades reales.

Factores de cegado (blinding factors). Funcionan como claves privadas adicionales que multiplican los montos y garantizan que solo los participantes de la transacción conozcan los números reales involucrados.

CoinJoin integrado. Agrupa múltiples transacciones en un solo bloque complejo, eliminando los historiales individuales y rompiendo el vínculo directo entre las direcciones de origen y destino.

Direcciones furtivas (stealth addresses). Permiten que el remitente genere, para cada transacción, una dirección de recepción única y privada para el destinatario, evitando que esta se reutilice o se mapee públicamente.

Pruebas de exceso cero (excess values). La red verifica que la suma de los compromisos de salida, menos los de entrada, sea igual a cero (o a las comisiones de los mineros), validando la contabilidad general de la cadena mediante criptografía de curva elíptica, sin exponer los datos subyacentes.

Riesgos en mixers y protocolos DeFi

La descentralización de los servicios financieros ha permitido la creación de herramientas legítimas de privacidad que, al mismo tiempo, representan un alto riesgo operativo debido a su explotación por parte de actores maliciosos.

Mezcladores de criptoactivos (mixers / tumblers). Servicios —basados en servidores centralizados o en contratos inteligentes no permisionados, como Tornado Cash— que agrupan depósitos de múltiples usuarios, mezclan los activos dentro de un fondo común de liquidez (liquidity pool) y permiten retiros hacia direcciones completamente nuevas y limpias. La ruptura del vínculo se

logra porque el retiro se autoriza mediante una prueba criptográfica (nota de depósito) que no guarda correlación indexable con la dirección de origen.

Protocolos de préstamo DeFi (decentralized lending). Una tipología avanzada de ocultamiento consiste en depositar criptoactivos de origen ilícito como colateral en un protocolo de préstamos, como Aave o Compound, para retirar un activo diferente en forma de préstamo, por ejemplo, una stablecoin. El investigador se encuentra entonces ante un flujo de fondos en el que el dinero de salida está respaldado por una deuda legítima del protocolo, lo que encubre el flujo ilícito subyacente que actúa como garantía latente.

Anatomía técnica de Tornado Cash

Tornado Cash se define técnicamente como un protocolo descentralizado y no custodial de mezcla de criptomonedas (mixer) que utiliza la criptografía zk-SNARK (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) para permitir transacciones privadas. A diferencia de los mezcladores tradicionales de primera generación, que requerían confiar la custodia de los fondos a un operador centralizado —introduciendo riesgos de robo o incautación—, Tornado Cash opera mediante contratos inteligentes inmutables.

El usuario deposita fondos en el contrato y recibe una «nota» criptográfica o un secreto; posteriormente, utiliza esa nota para demostrar matemáticamente que tiene derecho a retirar fondos, sin revelar a qué depósito específico corresponde.

Fundamentos criptográficos: zk-SNARK

Un aspecto fundamental de Tornado Cash es la tecnología zk-SNARK. Para el investigador forense, comprender este concepto es crucial, porque explica por qué el rastreo directo es matemáticamente inviable, y no simplemente difícil.

Zero-Knowledge (conocimiento cero). El protocolo permite verificar la validez de una transacción sin revelar ninguna información sobre esta, como el origen de los fondos. El verificador, o el contrato inteligente, sabe que la afirmación es verdadera, pero no conoce los datos que la hacen verdadera.

Non-Interactive (no interactivo). No se requiere un proceso de comunicación de ida y vuelta entre el probador (usuario) y el verificador; el usuario envía una sola prueba, suficiente para la validación.

Argument of Knowledge (argumento de conocimiento). Es una garantía computacional de que el probador realmente posee la información secreta (la nota) y no se encuentra simplemente adivinando.

En la práctica, cuando un usuario interactúa con Tornado Cash, no está «mezclando» sus monedas con las de otros en el sentido físico de revolverlas. Más bien, deposita su activo en una caja fuerte común y recibe un recibo criptográfico. Al retirar, presenta una prueba zk-SNARK que convence al contrato de que posee un recibo válido no gastado, sin revelar cuál recibo específico es. Esto disocia la dirección de depósito de la dirección de retiro.

Estructura de datos: el árbol de Merkle

Para gestionar los depósitos de manera eficiente y privada, Tornado Cash utiliza un árbol de Merkle incremental.

Cada depósito se convierte en una «hoja» (leaf) dentro de este árbol.

La hoja no contiene los datos del usuario en texto plano, sino un «compromiso» (commitment), resultado de aplicar una función hash a un secreto generado por el usuario.

El contrato inteligente mantiene el historial de las raíces (roots) del árbol de Merkle. Cuando un usuario desea retirar fondos, debe demostrar que su compromiso existe dentro de una de las raíces históricas válidas del árbol.

Variantes del protocolo: Classic frente a Nova

Es imperativo que el investigador distinga entre las dos arquitecturas principales de Tornado Cash, ya que presentan vectores de análisis forense distintos:

Tabla No. 9

Comparación entre Tornado Cash Classic y Tornado Cash Nova

Característica	Tornado Cash Classic	Tornado Cash Nova
Modelo de depósito	Montos fijos (0.1, 1, 10, 100 ETH).	Montos arbitrarios (cualquier cantidad).
Cadena principal	Ethereum Mainnet (y otras redes compatibles con la EVM).	Gnosis Chain (capa 2 / sidechain).
Riesgo forense	Menor, debido a la indistinguibilidad por monto.	Mayor, por el riesgo de correlación asociado a montos exactos.
Estado legal	Sancionado (sanción posteriormente levantada).	También afectado por las sanciones.

En Tornado Cash Classic, la rigidez de los montos constituye una característica de seguridad: si un usuario pudiera depositar, por ejemplo, 3.14159 ETH,

sería trivial rastrear ese monto único hasta la salida. Al forzar a todos los usuarios a emplear montos estándar, cada depósito de 10 ETH resulta idéntico a cualquier otro depósito de 10 ETH, lo que maximiza el conjunto de anonimato.

Tornado Cash Nova, por su parte, permite depositar y transferir fondos dentro del pool sin retirarlos (shielded transfers), operando de manera similar a Zcash mediante un modelo de salidas de transacción no gastadas (UTXO). Esto ofrece mayor flexibilidad, pero introduce complejidades adicionales en el análisis de metadatos.

La función primordial de Tornado Cash, tanto en el contexto del lavado de activos como en el de la privacidad legítima, es la ruptura del grafo de transacciones. En el análisis forense tradicional, las herramientas de trazabilidad siguen el flujo de activos de una dirección a otra; Tornado Cash interrumpe este flujo al insertar una «caja negra» criptográfica en la que la entrada es pública y la salida es pública, pero la conexión entre ambas resulta matemáticamente indetectable sin la clave privada (nota).

Conjunto de anonimato

El concepto central para medir la eficacia del ofuscamiento es el denominado «conjunto de anonimato» (anonymity set), definido como el grupo de todos los depósitos disponibles en el contrato inteligente en el momento de un retiro.

Si un usuario deposita en un pool que cuenta con otros noventa y nueve depósitos activos, la probabilidad de que un retiro específico corresponda a ese usuario es de 1/100, asumiendo una distribución uniforme y la ausencia de filtraciones de metadatos.

Cuanto mayor sea el conjunto de anonimato —es decir, cuantos más usuarios y depósitos se mantengan en el tiempo—, mayor será la ofuscación resultante. La privacidad en Tornado Cash es, por tanto, un bien colectivo: «la privacidad ama la compañía».

Indistinguibilidad criptográfica

El ofuscamiento se logra porque el contrato inteligente verifica la legitimidad del retiro sin necesidad de leer el origen de los fondos.

Desvinculación. Al retirar, el contrato verifica una prueba matemática que certifica que «el solicitante posee una nota válida X que corresponde a un depósito en el árbol Y», sin revelar cuál depósito específico es.

Prevención de doble gasto (nullifiers). Para evitar que un usuario retire el mismo depósito en múltiples ocasiones, el sistema utiliza «anuladores» (nullifiers). Al crearse un depósito se genera un anulador secreto; al retirar, el usua-

rio debe revelar el hash de ese anulador, y el contrato registra dicho hash. Si alguien intenta usar la misma nota nuevamente, el contrato detecta que el hash del anulador ya existe en su lista de «gastados» y rechaza la transaccións.

12 CIBERSEGURIDAD Y PROTECCIÓN DE ACTIVOS DIGITALES

12.1 Seguridad en wallets (Carteras Digitales)

Arquitectura de almacenamiento y separación de entornos: La protección de los activos digitales exige distinguir rigurosamente entre carteras conectadas a la red (hot wallets) y carteras desconectadas (cold wallets o almacenamiento en frío). Las primeras, orientadas a la liquidez operativa transaccional, deben contar con barreras de mitigación de riesgos y límites estrictos de saldo expuesto. Las segundas, destinadas al resguardo patrimonial de largo plazo, deben mantener las llaves privadas totalmente aisladas de internet mediante hardware especializado.

Mecanismos de autenticación y control de acceso: Implementación obligatoria de autenticación multifactor (MFA), verificación biométrica cuando aplique y protocolos de doble autorización para mitigar el riesgo de accesos no autorizados derivados de vulnerabilidades en los dispositivos de uso cotidiano.

12.2 Custodia institucional

Modelos de gobernanza corporativa y segregación de funciones: En estructuras organizacionales y fondos institucionales, la custodia de activos digitales no puede recaer en una sola persona. Se requiere un modelo de control interno basado en esquemas de multifirma (multisig) y contratos inteligentes de custodia institucional, donde las operaciones financieras significativas requieran la validación independiente de múltiples oficiales de cumplimiento o directivos.

Cumplimiento normativo y marco de control: Alineación con los estándares internacionales de gestión de riesgos tecnológicos y ciberseguridad, asegurando la trazabilidad absoluta de cada activo bajo custodia mediante libros de contabilidad distribuidos y registros de auditoría inmutables (audit trails).

12.3 Gestión de claves privadas

Ciclo de vida criptográfico: La clave privada representa el título ejecutivo y de propiedad indiscutible sobre el activo digital. Su pérdida o destrucción física o lógica implica la pérdida irreversible de los fondos. Los protocolos institucionales exigen procedimientos formales para su generación mediante generadores de números pseudoaleatorios seguros (CSPRNG).

Políticas de respaldo y secreto compartido: Obligatoriedad de respaldos físicos mediante frases semilla (seed phrases) cifradas, fragmentadas y distribuidas geográficamente bajo esquemas de división de secretos (por ejemplo, el algoritmo de Shamir), prohibiendo tajantemente el almacenamiento digital en texto plano, fotografías o nubes públicas sin cifrado extremo de conocimiento cero (zero-knowledge).

12.4 Riesgos de hacking y phishing

Tipologías de vectores de ataque: Identificación y monitoreo constante de amenazas avanzadas como ataques de suplantación de identidad (phishing, spear phishing), páginas web espejo fraudulentas, interceptación de portapapeles (clipboard malware) y vulnerabilidades en contratos inteligentes de terceros (smart contract exploits).

Programas de concientización y defensa humana: Establecimiento de simulacros periódicos y programas de capacitación continua para todo el personal con acceso a plataformas tecnológicas, orientados a la detección temprana de señales de alerta, verificación de firmas de transacciones y validación de canales de comunicación corporativos.

12.5 Incidentes de seguridad y respuesta forense

Activación de protocolos de contención y mitigación: Ante cualquier vulneración, brecha o sospecha de compromiso, se activa de forma inmediata el plan de respuesta a incidentes, aislando los nodos afectados para evitar la propagación horizontal del ataque hacia otros sistemas o carteras institucionales.

Cadena de custodia en soportes y dispositivos electrónicos: De acuerdo con los procedimientos formales de peritaje informático y auditoría forense, la recolección, aseguramiento y análisis de la evidencia digital (discos duros, servidores, dispositivos móviles y registros de blockchain) debe cumplir estrictamente con los principios de la cadena de custodia:

Identificación y registro in situ: Documentación detallada de la escena digital, número de serie, marcas temporales y estado de los dispositivos al momento de la intervención, fijando la evidencia mediante sellos de inviolabilidad.

Embalaje y transporte forense: Utilización de bolsas antiestáticas y contenedores blindados contra señales electromagnéticas (jaulas de Faraday) cuando se trate de dispositivos móviles activos, garantizando que no sufran alteraciones físicas ni remotas.

Adquisición forense de datos: Generación de copias bit a bit (forensic images) utilizando herramientas con funciones hash validadas criptográficamente (MD5 o SHA-256) para demostrar fehacientemente que la evidencia digital no ha sido modificada, garantizando su admisibilidad probatoria en procesos judiciales o administrativos.

12.6 Continuidad del negocio y recuperación digital

Planes de recuperación ante desastres (Disaster Recovery Plans - DRP): Diseño, documentación y pruebas periódicas de los planes de contingencia tecnológica para asegurar que la organización pueda restablecer sus operaciones críticas y el acceso a su infraestructura digital en plazos óptimos (Recovery Time Objective - RTO) minimizando la pérdida de datos (Recovery Point Objective - RPO).

Resiliencia operativa y auditorías de seguridad recurrentes: Evaluación continua de la postura de seguridad mediante pruebas de penetración (pentesting), auditorías de código fuente en desarrollos propios y revisiones exhaustivas de la arquitectura de red, garantizando una mejora cíclica frente al dinamismo de las amenazas cibernéticas globales.

PARTE V

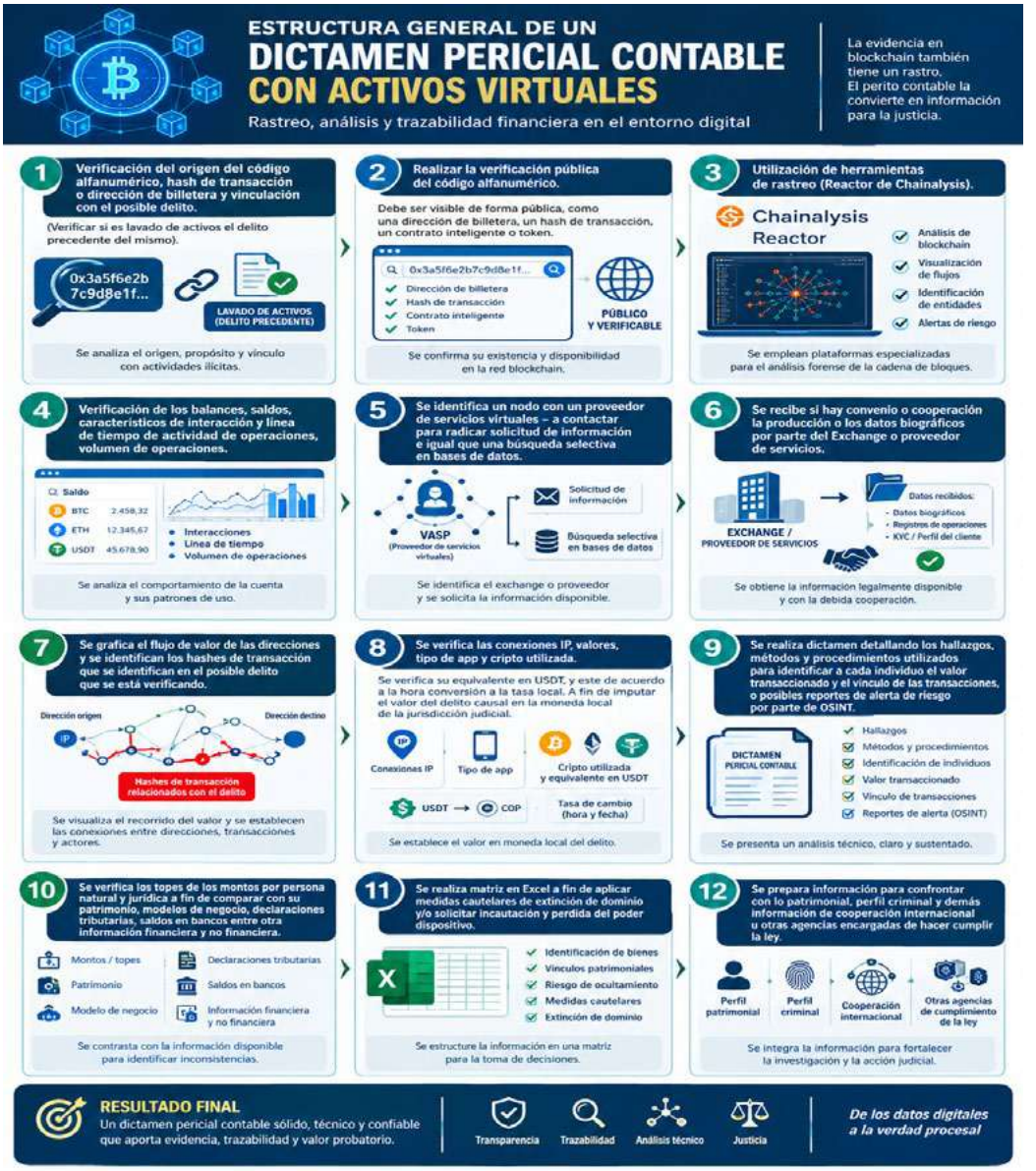
Peritaje Contable y Prueba Judicial

13 PERITAJE CONTABLE EN CRIPTOACTIVOS

El peritaje contable en cripto activos, cumple las mismas condiciones y características técnicas y jurídicas similares a un dictamen dentro de un proceso penal, administrativo, fiscal, disciplinario entre otros que requieran la aplicación de métodos, técnicas y ciencias auxiliares de la administración de justicia para la toma de decisiones imparciales y meramente tomadas desde un criterio profesional basado en una opinión pericial y en la correcta aplicación de métodos y otros que permiten la construcción de criterios con la capacidad técnica y que estos puedan ser primero, expuestos en audiencias y que los mismos puedan ser controvertidos o que se les pueda aplicar el principio de contradicción por su contraparte, aplicando los mismos criterios técnicos y metodológicos un profesional homologo deberá llegar a las mismas conclusiones.

Como se podría conocer de forma muy general, en todo el mundo por las agencias del orden o encargadas de hacer cumplir la ley, otras autoridades e instituciones al momento de incorporar algún elemento de este tipo "dictamen" a un juicio o para que una autoridad deba tomar decisiones en la posible materialización de un delito financiero y económico o de otra índole como lo podrían ser de financiamiento del terrorismo y/o armas de destrucción masiva, dentro de una investigación penal Interamericana o nacional que incorpora activos virtuales, toda vez que estos criterios, métodos y técnicas de auditoría forense no son nuevas, y se vienen aplicando por la gran mayoría de las diversas fuerzas del orden en el mundo, desde el año 2018, y antes de otras formas, pero es cuando se visualizó que esta tecnología emergente empezó a ser utilizada por un muy pequeño porcentaje de organizaciones criminales en el mundo, para la transferencia de valor y la necesidad de las autoridades para la identificación de la trazabilidad de valor dentro de los delitos transnacionales.

Estructura general de un dictamen pericial contable con activos virtuales: El perito contable convierte la información en decisiones para la justicia.



Verificación del origen del código alfanumérico, hash de transacción o dirección de billetera y vinculación con el posible delito (verificar si es lavado de activos el delito precedente del mismo)

Realizar la verificación pública del código alfanumérico debe ser visible de forma pública, como una dirección de billetera, un hash de transacción un contrato inteligente o token.

Utilización de herramientas de rastreo reactor de chainalysis

Verificación de los balances, saldos, característicos de interacción y línea de tiempo de actividad de operaciones, volumen de operaciones

Se identifica un nodo con un proveedor de servicios virtuales – a contactar para radicar solicitud de información igual que una búsqueda selectiva en bases de datos

Se recibe si hay convenio o cooperación la producción o los datos biográficos por parte del Exchange o proveedor de servicios.

Se grafica el flujo de valor de las direcciones y se identifican los hashes de transacción que se identifican en el posible delito que se está verificando.

Se verifica las conexiones ip, valores, tipo de app y cripto utilizada se verifica su equivalente en USDT, y este de acuerdo a la hora conversión a la tasa local. A fin de imputar el valor del delito causal en la moneda local de la jurisdicción judicial.

Se realiza dictamen detallando los hallazgos métodos y procedimientos utilizados para identificar a cada individuo el valor transaccionado y el vínculo de las transacciones, o posibles reportes de alerta de riesgo por parte de OSINT

Se verifica los topes de los montos por persona natural y jurídica a fin de comparar con su patrimonio, modelos de negocio, declaraciones tributarias, saldos en bancos entre otra información financiera y no financiera.

Se realiza matriz en Excel a fin de aplicar medidas cautelares de extinción de dominio y/o solicitar incautación y pérdida del poder dispositivo.

Se prepara información para confrontar con lo patrimonial, perfil criminal y demás información de cooperación Interamericana u otras agencias encargadas de hacer cumplir la ley.

13.1 Rol del perito contable especializado

El rol que debe cumplir un profesional certificado en investigaciones con activos virtuales, es a la final sencilla pero muy importante, debe garantizar un procedimiento debido de verificación y validación, tanto la tecnología como las transacciones de valor y es en este preciso momento que se realiza un trabajo armónico dentro de la aplicación interdisciplinaria de la auditoría forense entre el ingeniero de sistemas, perito en informática y el contador público perito en contabilidad forense y otras áreas del conocimiento, estos todos certificados, entrenados y con conocimiento y experiencia real en la investigación con activos virtuales.

Por qué partiendo de la casuística esta interdisciplinariedad de la auditoría forense, como siempre invita a que diversas áreas del conocimiento converjan en la recolección, análisis, comprensión y explicación de un fenómeno que re-

vista la características de delito ha traído mejor desarrollo en las audiencias de juicio oral en la exposición detallada técnica pero a la vez sencilla de primero la operación de la tecnología de como operan y la comprensión del comportamiento contable y el valor de la transacción.

El perito dentro de su rol debe tener claro que debe ir a audiencia de juicio oral, como testigo de acreditación a fin de atestar verbalmente la participación, le método y la técnica así como exponer de forma clara sus conclusiones e igualmente deberá prepararse para el interrogatorio al perito, toda vez que este interrogatorio se encuentra descrito dentro de los códigos penales y de procedimiento penal entre otros y se deberá tener claro su experiencia y la experticia para desarrollar estos procedimientos, su formación acreditación y entrenamiento.

13.2 Valor probatorio de blockchain

Una de las realidades más importantes, es el valor probatorio la no inmutabilidad de la blockchain y el libre acceso a su consulta, esta estructura también es importante explicarla ante un estrado judicial o un operador de justicia.

Es de resaltar que todas las transacciones de dólares digitales, criptomonedas o activos virtuales existentes, se realizan a través de la red BLOCKCHAIN, que es una tecnología que sin la intermediación de terceros, permite llevar a cabo transacciones digitales de forma rápida y descentralizada y las transacciones en activos digitales pueden rastrearse por cualquier ciudadano con acceso al internet; un explorador de bloques y las direcciones criptográficas están íntimamente relacionados: estas herramientas permiten inspeccionar las actividades de cualquier dirección pública en una blockchain.

Comprendiendo que Blockchain es una forma de registro o libro mayor utilizado por la mayoría de las criptomonedas y funciona encadenado por bloques de datos. Cada uno de los bloques contiene información acerca de la operación que se está realizando. Los elementos iniciales y finales del bloque se relacionan, haciendo extremadamente difícil su alteración y en algunos casos cada criptomoneda puede tener su propia red blockchain.

Muestra de un explorador de bloques y la capacidad de ser visible sin intermedio de terceros un pequeño ejemplo lo podemos hacer por medio de escanear el siguiente código QR.



Fuente: Explorador de bloque.

ejemplo: (https://blockchair.com/es/bnb/address/0xd8dA6BF26964aF9D7eEd9e03E53415D37aA96045)

En este se puede visualizar el has de dirección, el saldo en la criptomoneda y en USD e igualmente las transacciones recientes, con esta evidencia se le explica a el juez que es información que normalmente cualquiera puede ver, diferente a la desanonimización.

Un explorador de bloques es una herramienta que te permite buscar y ver datos registrados en una blockchain, como transacciones, balances de billetera y detalles de bloques.

Los exploradores de bloques funcionan como motores de búsqueda y ofrecen una forma fácil de usar para navegar por datos en la cadena que, de otro modo, serían difíciles de leer.

Cada blockchain tiene su propio explorador. Algunos ejemplos populares incluyen Mempool.space para Bitcoin, Etherscan para Ethereum, BscScan para BNB Chain y Solscan para Solana.

Los exploradores de bloques pueden ser útiles para verificar transacciones, rastrear la actividad de billeteras, revisar detalles de contratos inteligentes y entender mejor cómo opera una red blockchain.

Visualizamos un explorador de bloques de consulta pública, esta confirmación es de vital importancia por el acceso a la información al momento de desarrollar los análisis dentro del proceso para visualizar esa información no se requiere apoyo o solicitud de terceros o algún acceso a bases de datos en particular, teniendo en cuenta las normas procedimentales para algunos accesos debemos justificar la necesidad antes un juez y este autorizar la búsqueda y posteriormente formalizar de nuevo en audiencia los resultados de la misma. Es así que para el caso de validar la información de la cual se puede acceder sin intermediación de terceros hay que realizar la verificación de forma individual

dentro del proceso y esta información la podrá visualizar cualquier persona con acceso a internet en un dispositivo móvil.

13.3 Elaboración del dictamen pericial

La diferenciación de un informe normal a un dictamen pericial debe ser claro dentro del valor probatorio y dentro de la estructuración y conocimiento de los expertos, ya que este tiene diversas particularidades muy específicas y siempre esta detallada en la norma penal, procedimental, disciplinaria, administrativa y de extinción de dominio si para el país aplica. Entonces es basado en los requerimientos de ley para que este documento sea catalogado dictamen es que cumple sus requisitos, no solo por la realización por parte de un Perito idóneo, su estructura y la composición del informe debe tener como nimio en la mayoría de nuestros países la siguiente estructura.

Inicialmente la unidad pública o privada, a fin de tener un control y organización de la información, productos y servicios deberá asignar un consecutivo único al dictamen.

Seguidamente se deberá identificar este dictamen a que aporte procesal está vinculado, acá hablamos del número de expediente de investigación de auditoría, penal, disciplinario, contractual o el que aplique.

Deberá identificar el lugar geográfico, donde es desarrollado, fecha y hora y estos datos son importantes teniendo en cuenta que en la mayoría de los procesos existen términos perentorios que están medidos en días u horas hábiles, no debe existir un dictamen sin fecha y hora de presentación o finalización.

También el informe deberá dejar detalladamente quien o quienes lo elaboran, dirección, empresa y demás datos que permitan ubicar e identificar al equipo que desarrollo el encargo o dictamen, sin olvidar que los dictámenes o auditorías forenses pueden en debida forma ser realizada por equipos interdisciplinarios, estos podrán presentar un solo documento o documentos aparte según sus criterios profesionales.

El destino del informe debe ser claro, toda vez que se debe identificar el cliente a quien está construyéndose dicho dictamen, para casos procesales o penales será el despacho de la autoridad o el investigador líder dependiendo el caso y para un encargo litigioso será el abogado líder del proceso, para otros casos podrá ser el gobierno corporativo, debe en este punto estar claro por qué los profesionales pueden hacer parte de este procedimiento, porque media un contrato, porque media una orden de autoridad o cual sea que identifique la función de la autorización o la condición vinculante para el proceso.

El objetivo del dictamen este debe ser claro y definido, porque el dictamen deberá responder a este objetivo y no otras actividades, este objetivo deberá comprender la capacidad para recolectar la evidencia y la misma capacidad para procesarla, la línea de tiempo y las demás complejidades que pueda presentar el profesional al momento de plantear el objetivo del dictamen, estos también pueden ser sencillos como identificar y certificar un gobierno corporativo, trazabilidad del dinero, capacidad para adquirir bienes, incrementos en el patrimonio todos estos de personas naturales y jurídicas, dentro de este objetivo la individualización de objetivos debe ser congruente también ya que se debe identificar si es persona natural o jurídica o un establecimiento de comercio y los datos mínimos de identificación de estos y los tiempo o ventana de temporalidad del dictamen requerido, cuando hablamos de evaluar el crecimiento económico, algún posible delito financiero y económico debemos ubicarlo en una línea de tiempo, tomando un par de años anterior y/o posterior a los que se requiere verificar por medio de la auditoría forense en la elaboración del dictamen.

Los elementos tenidos en cuenta para el dictamen deben estar totalmente detallados de la forma en que la ley o los manuales permitan describir las evidencias, elementos materiales probatorios y evidencia física o información legalmente obtenida, y su tratamiento dando una validación inicial de su autenticidad y origen, no permitiendo su modificación, alteración o daño.

Deberán describirse y explicarse los métodos, principios y procedimientos técnicos que se utilizaran en el dictamen en particular y por más parecido todos son diferentes o puede aplicar métodos o técnicas diferentes y/o normatividad diferente y esto debe estar totalmente descrito para delitos financieros y económicos cobra relevancia las ciencias económicas y para el caso de activos virtuales el conocimiento dentro del ecosistema de criptoactivos.

Parte fundamental para un dictamen y donde la Asociación Interamericana de Contabilidad AIC – apoya mediante la construcción de sus manuales en Iberoamérica es la confirmación de la aceptación de los principios, métodos y procedimientos por parte de la comunidad técnico científica, equipos académicos, universidades y diversas teorías en el mundo que han confirmado la aceptación y aplicación de los métodos técnicas y procedimientos que se han seleccionado para la aplicación en el análisis de los elementos puestos a disposición para el dictamen.

Igualmente, al momento de utilizar equipos e instrumentos para el dictamen debemos describir claramente sus características y como fueron utilizados por el experto así mismo si estos requieren, calibración, actualización o licenciamiento debe confirmarse que estos estén en óptimas condiciones para la realización del dictamen pericial.

Exponer los resultados de forma técnica, profesional y detallada en cada uno de los pasos a pasos aplicados en el procesamiento de la evidencia.

Si bien es cierto ya en el punto anterior se expusieron los resultados del dictamen también debemos poner un punto final donde los resultados sean explicados, teniendo en cuenta que los resultados puedan contener lenguaje muy técnico que podría no permitir claridad en los administradores de justicia que no siempre tienen que ser expertos en otras áreas del conocimiento, deberá explicarse los resultados del dictamen en un lenguaje sencillo permitiendo una interpretación clara y fácil sobre las conclusiones del experto.

Se tendrá un punto para observaciones a fin de diligenciarlo debido el caso, identificar en este punto cualquier posible observación a presentarse durante la auditoría como: la falta de acceso a la información, que se accedió a la información, pero no es legible o esta dañada, entre otros.

También tendremos un aparte de anexos, todos los documentos o papeles de trabajo, graficas entre otros que el equipo de expertos considere mínimos para la operación.

Debe para finalizar el dictamen ser firmado, con su rúbrica y con todos los datos de notificación, dirección, correo electrónico, celular o teléfono, cedula o id del perito o experto – se deberá evaluar si tiene nombramiento, de lo contrario deberá anexar una copia de su hoja de vida, tarjeta profesional y experiencia sobre la pericia.

Utilización de herramientas de analítica investigativa como CRONIX



En diversos países de la región se cuentan con múltiples herramientas que permiten el tratamiento de datos y grandes volúmenes de información, es indispensable identificar cuáles y como pueden ser utilizadas cada una por separado y cuando pueden o es vital utilizarlas en conjunto es el caso de diversos equipos de soluciones tecnológicas como Altia, Reactor de Chainalysis, Notebook i2 y Cronix. La correcta aplicación y operación de estas permiten manejar volúmenes de investigación de más de 10 corporaciones 20 personas naturales hasta por los últimos 30 años. Debiendo analizar el total de la evidencia recolectada siendo esta información financiera y no financiera.

13.4 Técnicas de sustentación judicial

Una de las mejores sustentaciones en audiencias de juicio oral, es la explicación de forma clara y técnica. Pero permitiendo llevar a un lenguaje común la interpretación transaccional.

Igualmente debe estar claro la intervención de cada individuo y el monto que traslado, mediante que vehículo, tecnológico financiero y si este se ocultó o se materializo en otro lugar, mediante que técnica que método y que verbo rector del delito de aplico en su comportamiento en que línea de tiempo, cuantificando los valores para cada persona individual, por cierre de cada periodo ósea cada año y consolidado total por lo años del análisis.

Tener la información clara y los soportes jurídicos de la exposición, teniendo en cuenta que también es recomendable realizar una presentación de Power Point, sencilla donde se puedan proyectar los resultados, las gráficas de correlación, a fin de identificar los flujos de valor, los actores intervinientes y demás información relevante de la exposición del caso, del dictamen y del método criminal utilizado para materializar el delito financiero y económico entre otros delitos.

El perito deberá exponer con tranquilidad demostrando dominio del tema, la preparación del informe y el conocimiento de los procedimientos aplicados para la elaboración del dictamen, le servirán técnicas para hablar en público, una excelente presentación personal de nivel profesional, normalmente de traje formal para hombres y mujeres.

Trato respetuoso toda vez que el rito de la audiencia se trata de un mero acto de convencimiento del juez mediante la aplicación de los procedimientos de investigación, técnica, ciencia y método de los dictámenes periciales y la idoneidad del experto.

13.5 Estándares de evidencia digital

Los estándares mínimos Internacionales en materia de tratamiento de evidencia digital cobran una gran relevancia cuando tratamos de investigaciones con activos virtuales o auditorías forenses con este enfoque, ya que es prioritario la identificación del responsable de las transacciones y como en todo negocio muchas cosas pasan también como: falsifican documentos de identificación, realizan suplantación y utilizan la confianza de terceros para apertura productos, aunque algunos proveedores de servicios de internet cada día en el mundo y con el finde ganar credibilidad y minimizar los riesgos antijuridicos, realizan el conocimiento del cliente tomando pequeñas declaraciones desde el celular de las actividades comerciales o económicas y declaraciones de origen de fondos y validación del dispositivo de conexión así como la validación por medio de lecturas biométricas o fotografías y algunos documentos soportes de terceros como certificados de cuenta, recibos, pago de impuestos entre otros.

La evidencia digital relacionada con activos virtuales deberá ser tratada bajo los siguientes principios:

Autenticidad:

Integridad:

Trazabilidad:

Reproducibilidad:

Legalidad:

Corroboración Multifuente

Como principio diferenciador para las auditorías forenses sobre criptoactivos en Iberoamérica, ninguna conclusión relevante debería fundamentarse exclusivamente en una única fuente de información.

La evidencia blockchain deberá ser corroborada, siempre que sea posible, con otras fuentes independientes tales como:

- Información de proveedores de servicios de activos virtuales.
- Registros financieros y bancarios.
- Documentación contable.
- Evidencia informática.
- Información patrimonial.
- Fuentes abiertas de información.
- Registros públicos y corporativos.
-

14 COOPERACIÓN INTERAMERICANA Y RECUPERACIÓN DE ACTIVOS

14.1 Asistencia judicial Internacional

La naturaleza transnacional de los criptoactivos, las monedas digitales y las tecnologías blockchain ha transformado significativamente los procesos de auditoría forense, investigación financiera y recuperación de activos. A diferencia de los sistemas financieros tradicionales, los activos virtuales pueden movilizarse entre múltiples jurisdicciones en cuestión de segundos, interactuar con plataformas de diversos países y transferirse mediante infraestructuras tecnológicas descentralizadas sin que existan fronteras físicas para su circulación.

Por esta razón, las auditorías forenses relacionadas con activos virtuales exigen mecanismos de cooperación Interamericana eficaces que permitan intercambiar información, identificar beneficiarios finales, asegurar evidencia digital, ejecutar medidas cautelares y facilitar la recuperación de activos ubicados o administrados en jurisdicciones extranjeras.

La cooperación Interamericana constituye un elemento fundamental para reducir los riesgos derivados de la fragmentación jurisdiccional y fortalecer la capacidad de las autoridades, organismos de control, entidades fiscalizadoras, auditores forenses e investigadores financieros para rastrear operaciones complejas que involucren ecosistemas digitales globales.

Para estos procedimientos de auditoría forense con activos virtuales o algunos similares, teniendo en cuenta que su interpretación jurídica interna también puede variar un poco en la reglamentación regional, parte de estos procedimientos dependen de las funciones que tenga la institución que pretende ser beneficiaria de la cooperación Interamericana, normalmente utilizado en primera parte por los miembros del grupo EGMON o las Unidad es Inteligencia Financiera del Mundo, estas pueden realizar intercambio de información desde su función de inteligencia y dentro de las capacidades de cada país, igualmente algunas agencias encargadas de hacer cumplir la ley especialmente las fiscalías o ministerios públicos, entidades encargadas de llevar la carga de responsabi-

lidad penal y las técnicas de investigación que deberán realizarse en diversos países siempre será en coordinación de la cooperación Interamericana de las fiscalías o los ministerios públicos y apostillado por las cancillerías, a fin de que estas piezas procesales y otras técnicas tengan el debido rito jurídico para una imputación de cargos dentro del proceso penal o que su información de inteligencia pueda ser utilizada como referencia de indicio para el inicio u apertura de una investigación, como mecanismos de cooperación formal entre Estados.

14.2 Intercambio de información financiera

Mediante estos mecanismos de cooperación formal, las entidades encargadas de realizar la auditoría forense podrán entre otros tener acceso a obtención de registros de cuentas, información KYC y debida diligencia, identificación de beneficiarios finales, información de dispositivos de acceso, historial de transacciones, registros de custodia, información corporativa, antecedentes o ejecución de medidas cautelares, aseguramiento de activos virtuales o congelamientos preventivos.

14.3 Embargo, decomiso y medidas cautelares de activos virtuales

Partiendo de la aplicación procedimental de una investigación revestida con autoridad, territorialidad y funciones específicas para aplicación de cualquier medida de afectación de bienes dentro de procesos penales y/o administrativos estas deberán siempre propender por el principio de contradicción que en resumen significa que el afectado de la medida pueda apelar y de acuerdo con las diversas cargas dinámicas de la prueba, pueda presentar requerimientos para sustentar sus requerimientos. Las entidades con capacidad para aplicar estas medidas son:

- Unidades de Inteligencia Financiera.
- Fiscalías o Ministerios Públicos.
- Autoridades judiciales.
- Autoridades tributarias.
- Autoridades reguladoras financieras.
- Organismos de supervisión de activos virtuales.
- Organismos Internacionles de cooperación.

14.4 Recuperación Interamericana de criptoactivos

Para la recuperación de activos Interamericana, procedimiento normalmente aplicado en aplicación de cooperación Interamericana por las policías o agencias del mundo, como también litigios Internacionales entre diversos negocios Internacionales, deberán hacer uso de las capacidades de la estructura de negocio para realizar su recuperación en el sector privado deberán existir causales de conciliación y arbitraje Interamericana para blindar jurídicamente los negocios y convenios, así mismo las agencias del orden por intermedio de INTERPOL, presentan un programa piloto conocido como la Circular Plateada, donde su objetivo principal es la ubicación de activos tangibles e intangibles en diversos territorios de una persona natural y jurídica.

14.5 Coordinación con autoridades regulatorias

Las coordinaciones con diversas autoridades deberán medirse mediante convenios interadministrativos donde definan la claridad, alcance y necesidad del intercambio de información, mucha de estas para potencializar los negocios descentralizados o mixtos y otras para la aplicación de medidas preventivas en la evaluación del riesgo en los diversos ecosistemas que convergen en la transferencia de activos de valor, el conocimiento del cliente y la validación con información adicional, como lo suele ser el sistema financiero, el tributario, registradurías, migración entre otros.

PARTE VI

Casos Prácticos y Guías Metodológicas

15 CASOS DE ESTUDIO Y ANÁLISIS APLICADO

15.1 Casos reales Internacionales

Aquí se busca mostrar fraudes que trascendieron y cambiaron normativas.

Análisis forense de casos Wirecard, FTX, Petrobras y 1MDB. Identificación de fallas de control y metodologías de auditoría aplicadas.

Caso 1: Wirecard AG - Alemania 2020

Qué pasó: Faltaban 1.900 millones de euros en cuentas. El CFO ocultó saldos con empresas "fantasma" en Asia.

Falla: Auditor externo no validó terceros, gobierno corporativo débil, sobre confianza en crecimiento.

Metodología aplicada: Confirmaciones bancarias directas, pruebas sustantivas sobre terceros relacionados, análisis de flujo de caja vs utilidad.

Caso 2: FTX - Estados Unidos 2022

Qué pasó: Uso indebido de fondos de clientes para cubrir pérdidas de Alameda Research. Falta total de segregación.

Falla: No había consejo independiente, no había auditoría externa confiable, control de una sola persona.

Metodología aplicada: Revisión de custodia de activos, confirmación con blockchain explorers, pruebas de segregación de funciones.

Caso 3: Petrobras - Brasil 2014 "Lava Jato"

Esquema: Sobrefacturación de obras. 3% de cada contrato iba a corrupción. Lavado vía offshores y cuentas en USD.

Tipología impositiva: Facturas ideológicas, subfacturación de exportaciones, precios de transferencia.

Lección para auditor externo: Nunca confiar solo en documentos. Validar "sustancia sobre forma". Visitar obras, cruzar con proveedores reales.

Caso 4: 1MDB - Malasia 2015

Esquema: Desvío de 4.500 millones USD de un fondo soberano. Compra de arte, inmuebles, películas.

Tipología: Uso de sociedades offshore + bancos corresponsales + cripto para mover fondos.

Lección: Importancia del Beneficiario Final y Due Diligence de PEPss.

Guía metodológica: Para analizar casos Interamericanaes usar el modelo C.O.S.O. + enfoque en "Banderas Rojas": crecimiento excesivo, falta de transparencia, CEO dominante.

15.2 Fraudes corporativos con criptoactivos

Las cripto son el nuevo vector de fraude por su pseudonimato.

Tipologías más comunes:

Ponzi con criptomonedas:

Prometer rendimientos fijos. Ej.: Bitconnect 2017. Usaban nuevos inversionistas para pagar a los antiguos.

Desvío de tesorería a wallets personales: Directivos transfieren BTC/ETH de la empresa a billeteras propias. Difícil rastrear sin KYC.

Falsificación de volúmenes - Wash Trading: Inflar volumen en exchanges para atraer inversores.

Guía metodológica para auditoría:

Paso 1: Identificar todas las wallets de la empresa. Pedir listado + firmas.

Paso 2: Rastrear en Blockchain Explorer: Etherscan, BscScan. Ver movimientos a exchanges o wallets desconocidas.

Paso 3: Validar custodios. ¿Está en exchange regulado o en cold wallet con multifirma?

Paso 4: Cruce contable: Saldo en libros vs saldo en blockchain a fecha de cierre.

Banderas Rojas: Transferencias a mixers, uso de privacy coins sin justificación, falta de política de criptoactivos.

Tipologías: Ponzi, desvío de tesorería, wash trading.

Procedimientos de auditoría Impositiva: validación de wallets, conciliación blockchain vs contabilidad, riesgos tributarios. Marco legal Paraguay Ley 6.981/22.

Guía para Auditoría Impositiva

Riesgos Tributarios con Cripto:

Omisión de ingresos: Venta de BTC no declarada. El fisco ya cruza datos con exchanges.

Gastos no deducibles: Compra de cripto sin respaldo para "sacar" utilidades.

Precios de transferencia: Empresas que facturan servicios a offshore pagando en USDT.

Procedimientos de Auditoría Sugeridos:

Requerir: Declaración jurada de tenencia de criptoactivos al cierre.

Cruzar: Extractos bancarios vs movimientos en P2P como Binance P2P, Airtm.

Valuar: Usar cotización al 31/12 según BCP o fuente oficial. Diferencia de cambio.

Paraguay: Recordar que desde 2022 con Ley 6.981 hay regulación de criptoactivos. SEPRELAD pide registro a exchanges.

15.3 Investigaciones de lavado de activos

Basado en las 40 Recomendaciones del GAFI.

Caso aplicado: Esquema de "pitufeo" + facturas falsas

Esquema: Empresa deposita montos menores a 10.000 USD en varias cuentas. Luego compra cripto P2P y envía al exterior.

Falla de control: No se monitoreaban transacciones fraccionadas, no se hacía debida diligencia de clientes.

Metodología de investigación - 5 pasos:

Recolección: Extraer datos de ERP, bancos, correos. Cadena de custodia.

Análisis transaccional: Usar software tipo ACL, IDEA. Buscar picos, operaciones circulares, partes relacionadas.

Análisis de red: Mapear beneficiarios finales. ¿Quién está detrás?

Tipificación: Encausar según Ley 6524/20 de Paraguay. ¿Encaja en lavado?

Reporte: ROS a SEPRELAD + Informe para Directorio con recomendaciones.

Indicadores de alerta: Proveedores nuevos con pagos altos, facturas sin respaldo físico, empleados con estilo de vida incompatible.

Sugerencia Investigaciones de lavado de activos:

modelo de 6 fases:

Planeación: Entender el negocio. Matriz de riesgo LA/FT.

Identificación: Data Analytics. Reglas: "Transacciones >50.000 USD", "Proveedores con menos de 6 meses".

Recolección de Evidencia: Cadena de custodia digital. Hash de archivos.

Análisis: Triángulo del fraude + Diamante del fraude.

Conclusión y Tipificación: ¿Encaja en Art. 196 del Código Penal Paraguayo?

Comunicación: Informe ejecutivo + ROS a SEPRELAD si corresponde.

Caso Paraguay: Incluir referencia a Operativo "Berilo" o casos de frontera. El contrabando + lavado es muy común en **C.D.E.**

15.4 Auditorías internas y compliance

Cómo debe actuar el área para prevenir estos casos.

Guía metodológica de Auditoría Interna:

Enfoque basado en riesgos

Matriz de riesgo con peso a cripto, terceros, pagos Internacionales.

Pruebas clave:

Segregación de funciones en tesorería

Revisión de excepciones en sistema

Pruebas sorpresa de caja y wallets

Revisión de programa de Compliance: Código de ética, canal de denuncias

Programa de Compliance efectivo:	
Pilar	Qué debe tener
Tone at the Top	Directorio comprometido
Políticas	PLA/FT, Anticorrupción, Criptoactivos
Capacitación	2 veces al año mínimo
Monitoreo	KPIs: N° de alertas, N° de casos cerrados

Normas:

NIA 240: Responsabilidad del auditor en fraudes

NIA 315: Identificación y valoración de riesgos

ISO 37301: Sistema de Gestión de Compliance

COSO 2013: Control Interno

GAFI: 40 Recomendaciones

Checklist para Auditor Externo Impositivo:

¿Existe política de PLA/FT aprobada por Directorio?

¿Se auditan las operaciones con paraísos fiscales?

¿Hay canal de denuncias y se investiga?

¿Se concilian libros contables vs declaraciones juradas?

15.5 Lecciones aprendidas

No hay control infalible sin cultura: La tecnología ayuda, pero si el "tono de arriba" es malo, todo falla.

La auditoría debe actualizarse: Hoy no basta auditar caja y banco. Hay que auditar wallets, Smart contracts y exchanges.

Documentar todo: En fraude, el papel manda. Correos, actas, aprobaciones.

Prevención cuesta menos que corrección: Invertir en compliance evita multas, daño reputacional y cárcel.

Colaboración: Auditoría + Compliance + Jurídico + TI deben trabajar juntos.

Recomendaciones para Latam

Convergencia de riesgos: Fraude + Lavado + Cripto ya vienen juntos. El auditor debe ser multidisciplinario.

Tecnología: Usar ACL, IDEA, Power BI. Sin data analytics hoy no hay auditoría.

Importancia del Juicio Profesional: Ningún software reemplaza el escepticismo.

Cooperación Interinstitucional: AIC, SEPRELAD, SET, MP deben compartir tipologías.

Ética: El mejor control sigue siendo la integridad del auditor.

Conclusión del capítulo

Los casos demuestran que el fraude evoluciona. Ayer era en efectivo, hoy es en cripto. La metodología del auditor debe evolucionar también: más analítica de datos, más entendimiento de tecnología y más escepticismo profesionals.

Cómo debe actuar el área para prevenir estos casos.

Guía metodológica de Auditoría Interna:

Enfoque basado en riesgos:

Matriz de riesgo con peso a cripto, terceros, pagos Internacionales.

Pruebas clave:

Segregación de funciones en tesorería

Revisión de excepciones en sistema

Pruebas sorpresa de caja y wallets

2. Revisión de programa de Compliance: Código de ética, canal de denuncias

Conclusiones y recomendaciones para la región.

Importancia de la tecnología, el juicio profesional y la cooperación interinstitucional.

16 GUÍAS PRÁCTICAS PARA EL AUDITOR FORENSE (ACTIVOS VIRTUALES Y CRIPTOMONEDAS)

16.1 Checklists de Auditoría

Checklist A: Planificación e Identificación de Entornos Cripto

[Alcance de la investigación: Definición de la ventana temporal, entidades relacionadas y tipo de activos virtuales involucrados (Bitcoin, Altcoins, Stablecoins, Tokens ERC-20/SPL, NFTs).

Identificación de Puntos de Entrada/Salida (Fiat On/Off Ramps): Mapeo de cuentas bancarias corporativas/personales vinculadas a Exchanges centralizados (CEX) y Proveedores de Servicios de Activos Virtuales (PSAV/VASP).

Inventario de Claves y Custodia: Registro de direcciones públicas (Public Keys), tipo de custodia (Hot/Cold Wallets, custodial, no custodial, multisig) y responsables designados de la tenencia.

Checklist B: Adquisición y Preservación de Evidencia Cripto-Forense

Cadena de Custodia Digital: Emisión de la hoja de custodia para cada dispositivo físico (Hardware Wallets tipo Ledger/Trezor, servidores, móviles).

Extracción Forense On-Chain: Captura de hashes de transacción (TxIDs), block height, direcciones de origen/destino y metadatos del ledger distribuido.

Extracción Forense Off-Chain: Preservación de logs de acceso (direcciones IP, registros API, marcas de tiempo UTC), correos de confirmación de depósitos/retiros y credenciales/sesiones de Exchanges.

Integridad Algorítmica: Generación de valores Hash (SHA-256) sobre la totalidad de los archivos de evidencias capturados.

Checklist C: Trazabilidad y Reconciliación Financiera

Reconciliación Contable-Blockchain: Saldo en cadena de bloques vs. registros en libros contables tradicionales (cuenta contable de activos intangibles/financieros).

Rastreo de Técnicas de Opacidad: Identificación de uso de *mixers/tumblers* (Tornado Cash, CoinJoin), *Cross-Chain Bridges* (saltos entre blockchains) o *Privacy Coins* (Monero, Zcash).

Verificación KYC/AML: Obtención de información de titularidad formal mediante requerimientos legales a VASP centralizados.

16.2 Matrices de Riesgo

Matriz de Riesgo de Fraude y Lavado de Dinero mediante Activos Virtuales

Categoría de Riesgo	Amenaza Forense / Tipología Cripto	Probabilidad	Impacto	Mecanismo de Control y Mitigación
Opacidad Operativa	Uso de *Mixers*, *Bridges* o criptomonedas de privacidad para romper la cadena de trazabilidad del dinero ilícito.	Alta	Crítico	Empleo de herramientas de análisis analítico *on-chain* (Chainalysis, Elliptic) y seguimiento de heurísticas de agrupación (*clustering*).
Gobernanza y Custodia	Desvío no autorizado de fondos por acceso no restringido a la frase semilla (*Seed Phrase*) o ausencia de esquemas multifirma (*Multisig*).	Media	Crítico	Implementación de billeteras *Multisig* (m-de-n), custodia en *Hardware Security Modules* (HSM) y separación de funciones.
Valoración e Integridad	Manipulación de precios en libros mediante cotizaciones arbitrarias en *Exchanges* sin liquidez o transacciones simuladas (*Wash Trading*).	Alta	Alto	Validación de precios históricos frente a *Oráculos* descentralizados de referencia y promedios ponderados de volumen de mercado (VWAP).

Categoría de Riesgo	Amenaza Forense / Tipología Cripto	Probabilidad	Impacto	Mecanismo de Control y Mitigación
Incumplimiento Regulatorio	Transacciones con PSAV/VASP no registrados o direcciones sancionadas (listas OFAC, CSNU).	Media	Alto	Filtrado de direcciones *on-chain* mediante motores de *Risk Scoring* y listas de alerta automatizadas.

16.3 Modelos de Entrevistas Forenses

Guión Estructurado de Interrogatorio Técnico Forense

1. Fase de Contextualización y Perfil Técnico del Entrevistado:

"¿Cuál es su responsabilidad directa respecto al manejo de los activos virtuales dentro de la entidad?"

"¿Qué capacitación técnica posee sobre la operación de la tecnología Blockchain y administración de billeteras?"

2. Fase de Gestión de Claves y Operatividad:

"¿Dónde se encuentran físicamente almacenadas las frases semilla (semilla de recuperación de 12/24 palabras) y las claves privadas de las billeteras institucionales?"

"¿Quiénes poseen autorización técnica y firma digital para aprobar y emitir una transacción desde la billetera de la empresa?"

"¿Cuál es la política formal de la empresa para autorizar pagos o transferencias en criptoactivos a proveedores o terceros?"

3. Fase de Contraste con Evidencia *On-Chain*:

"El día [Fecha] a las [Hora UTC], la dirección pública de la empresa envió [Monto] en [Activo] al TxID [Hash]. ¿Podría explicar la justificación comercial de esa transacción y quién la autorizó?"

"Los registros muestran que dichos fondos terminaron en un servicio de mezcla (Mixer). ¿Por qué razón técnica se utilizó esta herramienta para procesar la operación?"

4. Fase de Cierre:

Ratificación de la declaración, firma del acta de entrevista forense y fijación de anexos documentales.

16.4 Formatos de Documentación Técnica

Estructura Normalizada del Informe Pericial Forense sobre Criptoactivos

INFORME DE AUDITORÍA FORENSE DE CRIPTOACTIVOS

==========

1. RESUMEN EJECUTIVO
   1.1. Objeto de la investigación
   1.2. Mapeo del perjuicio económico (Cuantificación en Fiat y en Criptoactivos)
   1.3. Conclusión pericial sintética
2. ALCANCE Y NORMATIVA DE APLICACIÓN
   2.1. Estándares aplicados (Normas AIC, NIA 240, ISO/IEC 27037 sobre Evidencia Digital)
   2.2. Período objeto de la pericia y direcciones de billetera analizadas
3. EVIDENCIA DIGITAL Y CADENA DE CUSTODIA
   3.1. Dispositivos físicos intervenidos y su Hash de verificación (SHA-256)
   3.2. Metodología de extracción de datos On-Chain (Blockchain) y Off-Chain (VASP/Servidores)
4. ANÁLISIS TÉCNICO Y TRAZABILIDAD (FORENSIC ON-CHAIN ANALYSIS)
   4.1. Origen, ruta y destino de los fondos (Flujograma de TxIDs)
   4.2. Identificación de patrones de centrifugación, peeling chains o uso de mixers
   4.3. Identificación de contrapartes y entidades (VASP de destino / KYC)
5. EVALUACIÓN DE CONTROLES E IMPUTABILIDAD
   5.1. Vulneraciones a la política de custodia de claves
   5.2. Determinación de responsabilidades operativas y técnicas
6. CONCLUSIONES PERICIALES Y PUNTOS DE PERICIA
   6.1. Respuestas detalladas a las preguntas formuladas por la parte solicitante / Tribunal
7. ANEXOS TÉCNICOS
   - Hoja de Cadena de Custodia
   - Reportes gráficos de trazabilidad on-chain (Chainalysis/Elliptic/Breadcrumbs)
   - Transcripción de eventos y smart contracts analizados

16.5 Indicadores de Alerta Temprana

Alertas Tecnológicas y *On-Chain* (*Red Flags*)

Patrón de "Peeling Chains": Transferencias sucesivas donde se envía una pequeña fracción a una dirección de destino y el resto a una nueva dirección de cambio controlada por el mismo usuario, repetido de forma automatizada.

Transacciones fuera de Horario Habitual: Movimientos significativos de fondos en fines de semana o madrugadas desde billeteras de la empresa sin previo aviso operativo.

Uso de Contratos Inteligentes Sin Auditar: Interacción de fondos corporativos con protocolos *DeFi* (Finanzas Descentralizadas) no verificados o de reciente creación.

Concentración de Transacciones bajo Umbrales: Múltiples depósitos o retiros justo por debajo del límite que activa los controles KYC o de reporte de operaciones en el VASP (*Structuring / Smurfing*).

Alertas Administrativas y *Off-Chain* (*Red Flags*)

Modificaciones imprevistas en los parámetros de la billetera multifirma (eliminación de firmantes clave o reducción del umbral de firmas requeridas m-de-n).

Negativa o evasivas del personal clave para entregar los respaldos o credenciales de acceso a las *Hardware Wallets*.

Incoincidencia entre la fecha/monto del registro contable de egreso en libros y el estampado de tiempo (*timestamp*) en la cadena de bloques.

16.6 Protocolos de Actuación Profesional

PROTOCOLOS DE ACTUACIÓN FORENSE

Protocolo 1: Reacción Inmediata ante Incidente o Fraude en Ejecución:

Notificación urgente y confidencial al Consejo de Administración / Comité de Auditoría.

Ejecución de revocación de aprobaciones de *Smart Contracts* mediante herramientas de emergencias y cambio inmediato de esquemas de clave privada.

Aislamiento físico de los dispositivos que contienen la infraestructura de billeteras (*Hardware Wallets* y terminales de firma) en bolsas Faraday para evitar manipulación remota.

Protocolo 2: Preservación de la Reserva (*Anti Tipping-Off*):

Guardar absoluta confidencialidad sobre la marcha del peritaje, asegurando que las indagaciones *on-chain* no alerten a los presuntos implicados para prevenir el movimiento de fondos hacia *mixers* o el borrado irrecuperable de las claves de acceso.

Protocolo 3: Escalamiento e Interacción Judicial / Regulatoria:

Empaquetado de la evidencia digital bajo la norma ISO/IEC 27037.

Redacción del Reporte de Operación Sospechosa (ROS) o colaboración en la formulación de la querella penal, adjuntando la trazabilidad de los *TxIDs* y el mapeo de los *Exchanges* receptores para facilitar órdenes judiciales de congelamiento (*freezing orders*)s.

PARTE VII

Prospectiva y desafíos futuros

17 TENDENCIAS EMERGENTES DE LA AUDITORÍA FORENSE

17.1 Introducción

La auditoría forense se encuentra en un proceso de transformación derivado de la digitalización de las operaciones financieras, la expansión de los activos virtuales, el desarrollo de la inteligencia artificial (IA) y la utilización de tecnologías de registro distribuido, como Blockchain. Estas innovaciones han modificado tanto las modalidades de comisión del fraude como los mecanismos disponibles para su prevención, detección, investigación y obtención de evidencia.

En este contexto, el auditor forense debe ampliar sus competencias tradicionales de análisis contable y financiero hacia el manejo de herramientas de análisis de datos, trazabilidad de activos virtuales, ciberseguridad, inteligencia artificial y evidencia digital. El objetivo ya no consiste únicamente en reconstruir operaciones después de ocurrido un hecho irregular, sino también en identificar patrones, relaciones y señales de alerta que permitan anticipar comportamientos potencialmente fraudulentos.

17.2 Inteligencia artificial y Blockchain

La integración de la inteligencia artificial y Blockchain constituye una de las principales tendencias tecnológicas con impacto en la auditoría forense. La IA proporciona capacidad de procesamiento, automatización, aprendizaje y detección de patrones, mientras que Blockchain permite registrar operaciones de manera trazable y resistente a modificaciones posteriores.

Esta combinación puede fortalecer significativamente los procesos de auditoría mediante:

Análisis automatizado de transacciones. La IA permite procesar grandes volúmenes de información financiera e identificar operaciones atípicas, relaciones inusuales y patrones potencialmente fraudulentos.

Monitoreo continuo. Los sistemas de IA pueden analizar transacciones en tiempo real y generar alertas ante comportamientos que se aparten de parámetros previamente establecidos.

Trazabilidad mediante Blockchain. La información registrada en una cadena de bloques puede facilitar la reconstrucción cronológica de determinadas operaciones y contribuir a la verificación de su integridad.

Contratos inteligentes. Los *smart contracts* permiten ejecutar automáticamente determinadas condiciones previamente codificadas, generando nuevos elementos que pueden ser objeto de revisión forense.

Análisis de riesgos. La combinación de IA y datos registrados en Blockchain puede contribuir a identificar relaciones entre personas, billeteras, transacciones y entidades involucradas en operaciones complejas.

Sin embargo, estas tecnologías también generan nuevos riesgos. Los modelos de IA pueden producir resultados incorrectos, sesgados o difíciles de explicar, mientras que la inmutabilidad de Blockchain no garantiza por sí misma que la información incorporada originalmente sea verdadera. Por ello, el auditor debe diferenciar entre la **integridad del registro** y la **veracidad de la información registrada**.

El FSB (2024) identifica, entre otros riesgos asociados con la IA, la dependencia de terceros, la concentración tecnológica, los riesgos de ciberseguridad, la falta de transparencia de determinados modelos y la posibilidad de que la IA sea utilizada para incrementar el fraude financiero.

17.3 Regulación futura de los activos virtuales

La expansión de los activos virtuales está impulsando la creación y fortalecimiento de marcos regulatorios en América Latina. La tendencia regional se orienta hacia una mayor identificación de los participantes del mercado, regulación de los proveedores de servicios de activos virtuales (PSAV/VASP), aplicación de medidas de prevención de lavado de activos y fortalecimiento de la supervisión.

En Argentina, la Comisión Nacional de Valores (CNV) incorporó un régimen específico para los Proveedores de Servicios de Activos Virtuales. La Resolución General N.º 1058/2025 desarrolló la reglamentación correspondiente, en el marco de las modificaciones introducidas por la Ley N.º 27.739.

Brasil constituye otro ejemplo relevante de evolución regulatoria. El Banco Central do Brasil emitió en noviembre de 2025 las Resoluciones BCB N.º 519, 520 y 521, mediante las cuales estableció procedimientos de autorización, regulación de los proveedores de servicios de activos virtuales y deter-

minadas disposiciones relacionadas con operaciones cambiarias y capitales Internacionales.

La regulación continuó desarrollándose durante 2026. El Banco Central de Brasil emitió nuevas disposiciones sobre supervisión, secreto financiero, atención al usuario y requerimientos prudenciales aplicables a las sociedades prestadoras de servicios de activos virtuales.

A nivel Interamericana, el FATF (2025) señala que persisten diferencias significativas en la implementación de los estándares aplicables a activos virtuales y proveedores de estos servicios. Estas diferencias pueden generar espacios de arbitraje regulatorio y facilitar el desplazamiento de actividades ilícitas hacia jurisdicciones con controles menos desarrollados.

Para el auditor forense, esta evolución implica la necesidad de conocer la normativa nacional e Interamericana aplicable, identificar la jurisdicción involucrada en cada operación y analizar la trazabilidad de los fondos entre entidades financieras, plataformas de activos virtuales y billeteras digitales.

17.4 Riesgos sistémicos y estabilidad financiera

La creciente interconexión entre los activos virtuales, las instituciones financieras tradicionales y las nuevas tecnologías genera riesgos que pueden trascender a una entidad individual y afectar la estabilidad del sistema financiero.

Entre los principales riesgos se encuentran:

Riesgo de contagio. Las pérdidas significativas en determinados mercados o plataformas pueden generar efectos sobre entidades financieras y otros participantes vinculados.

Riesgo de concentración tecnológica. La dependencia de un reducido número de proveedores tecnológicos puede generar vulnerabilidades operativas y sistémicas.

Riesgo algorítmico. El uso generalizado de modelos similares de IA puede provocar respuestas simultáneas ante determinados eventos y amplificar la volatilidad.

Riesgo de ciberseguridad. Los ataques dirigidos contra plataformas financieras, custodios o infraestructuras digitales pueden ocasionar pérdidas económicas y afectar la confianza del mercado.

Riesgo de liquidez y custodia. La falta de mecanismos adecuados de respaldo, administración o custodia puede dificultar la recuperación de activos ante eventos adversos.

El FSB (2024) identifica la concentración de proveedores, la dependencia de infraestructuras tecnológicas, la ciberseguridad y la utilización de IA como

factores que pueden incrementar determinadas vulnerabilidades del sistema financiero.

Por tanto, el auditor forense debe considerar que una investigación financiera moderna puede requerir analizar no solamente una operación aislada, sino también las relaciones existentes entre múltiples entidades, plataformas, usuarios y sistemas tecnológicos.

17.5 Evolución del crimen financiero digital

La transformación tecnológica también ha producido nuevas modalidades de delincuencia financiera. El fraude tradicional se ha complementado con mecanismos digitales capaces de operar a gran escala, con mayor velocidad y utilizando técnicas destinadas a dificultar la identificación de los responsables.

Entre las principales modalidades se encuentran:

- lavado de activos mediante activos virtuales;
- operaciones entre múltiples cadenas (*chain hopping*);
- utilización de billeteras no custodiadas;
- fraude mediante ingeniería social;
- suplantación de identidad mediante inteligencia artificial;
- utilización de *deepfakes*;
- ataques contra plataformas de activos virtuales;
- explotación de vulnerabilidades en contratos inteligentes;
- manipulación de información digital;
- utilización de inteligencia artificial generativa para automatizar estafas.

El FATF (2025) advierte sobre el incremento de la utilización ilícita de activos virtuales, incluyendo stablecoins, fraude y esquemas destinados a ocultar el origen de los fondos. Asimismo, durante 2025 el organismo identificó el uso creciente de inteligencia artificial generativa, agentes de IA y *deepfakes* como herramientas que pueden facilitar el fraude y otras actividades ilícitas.

El Fondo Monetario Interamericana también ha señalado la importancia creciente de los riesgos derivados de los eventos cibernéticos y del fraude digital para el sector financiero, lo que refuerza la necesidad de fortalecer las capacidades de prevención, detección y respuesta.

17.6 Nuevos desafíos para el auditor forense

El entorno digital exige que el auditor forense desarrolle competencias adicionales a las tradicionales. Los principales desafíos pueden resumirse de la siguiente manera:

Desafío	Impacto forense	Respuesta profesional
Volumen y velocidad de datos	La revisión manual resulta insuficiente.	Utilización de IA, minería de datos y análisis automatizado.
Anonimato y pseudonimato	Dificultan identificar al beneficiario real.	Análisis Blockchain y técnicas de trazabilidad de billeteras.
Evidencia digital	Puede ser modificada, eliminada o cuestionada.	Preservación, autenticación, *hash* y cadena de custodia.
IA generativa	Facilita suplantaciones y documentos falsificados.	Verificación independiente y análisis forense digital.
Contratos inteligentes	El fraude puede encontrarse en la lógica del código.	Revisión conjunta de operaciones, código y registros financieros.
Operaciones transfronterizas	Dificultan la investigación y recuperación de activos.	Cooperación Interamericana y análisis de múltiples jurisdicciones.
Cibercrimen	Integra fraude financiero y ataques tecnológicos.	Equipos interdisciplinarios de auditoría, ciberseguridad y derecho.

El auditor forense debe, por tanto, evolucionar desde una función centrada exclusivamente en la revisión histórica de documentos hacia un modelo basado en analítica avanzada, monitoreo continuo, investigación digital y evaluación de riesgos tecnológicos.

ANEXOS

Glosario técnico especializado

D. Formatos y modelos de trabajo de auditoría

ANEXO: No. 1

Ejemplo para modelo de trabajo para auditoría forense con activos virtuales, como papeles de trabajos.

Tabla No. 1 Anexo 1

Inventario de saldos de direcciones de billeteras virtuales su equivalente en USDT y el equivalente en su moneda local

No.	NOMBRES	DIRECCIÓN DE BILLETERAS VIRTUALES	SALDO ENERO a DICIEMBRE o SALDO DURANTE EL PERIODO DE EVALUACIÓN	PESOS TRM ejemplo: al cierre del 31/12/2021	SALDO	PESOS Moneda Local
	Nombre y apellido e	Código alfa numérico de las direcciones de billetera identificadas a su nombre o posible dominio	Saldo año a año del volumen transaccional al cierre del periodo de poder ser visible los periodos - de lo contrario cuantifica el total de las transacciones durante la duración	Valor del USDT - de la fecha de consulta o de la fecha periodo de los cierres de anualidad - TRM Tasa	Valor en USDT	Valor en la moneda local - para el caso de Colombia la conversión a pesos COL. (Toda vez que la imputación y

Creación:

Equipo interdisciplinario subcomisión para la construcción del Manual de Auditoría Forense Especializado en Criptoactivos, Moneda Digital y Blockchains.

Referencias

- Banco Central do Brasil. (2025, 10 de noviembre). *Resolução BCB nº 519, de 10 de novembro de 2025*. Banco Central do Brasil.
- Banco Central do Brasil. (2025, 10 de noviembre). *Resolução BCB nº 520, de 10 de novembro de 2025*. Banco Central do Brasil.
- Banco Central do Brasil. (2025, 10 de noviembre). *Resolução BCB nº 521, de 10 de novembro de 2025*. Banco Central do Brasil.
- Banco Central do Brasil. (2026, 26 de febrero). *Resolução CMN nº 5.280, de 26 de fevereiro de 2026*. Banco Central do Brasil.
- Banco Central do Brasil. (2026, 1 de julio). *Resolução BCB nº 580, de 1º de julho de 2026*. Banco Central do Brasil.
- Comisión Nacional de Valores. (2025, 12 de marzo). *Resolución General N.º 1058/2025: Reglamentación de proveedores de servicios de activos virtuales*. Comisión Nacional de Valores de Argentina.
- Financial Action Task Force. (2024). *Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers*. FATF.
- Financial Action Task Force. (2025). *Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers*. FATF.
- Financial Action Task Force. (2025). *Targeted report on stablecoins and unhosted wallets*. FATF.
- Financial Action Task Force. (2025). *Cyber-enabled fraud: Digitalisation, money laundering, terrorist financing and proliferation financing risks*. FATF.
- Financial Action Task Force. (2025). *Outcomes of the FATF plenary, 22–24 October 2025*. FATF.
- Financial Stability Board. (2024). *The financial stability implications of artificial intelligence*. FSB.
- International Monetary Fund. (2026). *The rise of cyber events and digital fraud in the financial sector*. International Monetary Fund.
- International Monetary Fund. (2025). *Financial integrity implications of retail central bank digital currencies*. International Monetary Funds.

Este documeto fue elaborado por sus autores y posteriormente revisado con apoyo de herramientas de inteligencia artificial para mejorar su redacción, coherencia y precisión técnica, entre esas Cloud, Gémini, Notebock LM, Chat gpt y Copilot. La revisión, validación de fuentes y responsabilidad sobre el contenido final corresponden a los autores.

BIBLIOGRAFÍA GENERAL

Referencias bibliográficas consolidadas de todos los capítulos del manual (Formato APA 7, orden alfabético, sin duplicados).

- Ahmed, R., Aldasoro, I., & Duley, C. (2024). Public information and stablecoin runs (BIS Working Papers No. 1164). Bank for International Settlements. [Versión revisada en enero de 2025].
- Aldasoro, I., Cornelli, G., Ferrari Minesso, M., Gambacorta, L., & Habib, M. M. (2024). Stablecoins, money market funds and monetary policy (BIS Working Papers No. 1219). Bank for International Settlements.
- Arriola, M. (2024). Blockchain y la evolución de la auditoría contable: Breve resumen de la investigación actual y reflexiones. https://doi.org/10.5281/zenodo.12707008
- Asociación Interamericana de Contabilidad, Comisión Interamericana de Peritaje Contable y Auditoría Forense. (2026). Manual de auditoría forense especializado en criptoactivos, moneda digital y blockchain. AIC.
- Association of Certified Fraud Examiners. (2024). Report to the nations: 2024 global study on occupational fraud and abuse. ACFE.
- Baer, K., de Mooij, R. A., Hebous, S., & Keen, M. (2023). Taxing cryptocurrencies (IMF Working Paper No. 2023/144). International Monetary Fund. DOI: 10.5089/9798400246586.001.
- Banco Central de Bolivia. Resolución de Directorio N.º 082/2024.
- Banco Central del Ecuador. (s. f.). Información sobre criptoactivos en Ecuador. https://www.bce.fin.ec/
- Banco Central del Paraguay. (s.f.). Comunicados y advertencias sobre activos virtuales y criptomonedas. https://www.bcp.gov.py/
- Bank for International Settlements & Committee on Payments and Market Infrastructures. (2024). Tokenisation in the context of money and other assets: Concepts and implications for central banks. BIS.
- Bank for International Settlements (BIS). The crypto ecosystem: key elements and risks, 2023.
- Bank for International Settlements. (2023). Blueprint for the future monetary system: Improving the old, enabling the new. En Annual Economic Report 2023, Chapter III. BIS.

- Bank for International Settlements. (2023). The crypto ecosystem: Key elements and risks. Report submitted to the G20 Finance Ministers and Central Bank Governors.
- Basel Committee on Banking Supervision. (2022). Prudential treatment of cryptoasset exposures. Bank for International Settlements. https://www.bis.org/bcbs/publ/d545.htm
- BIS. Cryptocurrencies and decentralised finance: functions and financial stability implications, 2025.
- Blockchair. (2026). Blockchain explorer and analytics. https://blockchair.com/
- Buterin, V. (2014). Ethereum: A next-generation smart contract and decentralized application platform. White paper.
- Committee of Sponsoring Organizations of the Treadway Commission. (2017). Enterprise risk management: Integrating with strategy and performance. COSO.
- Congreso de la República del Perú. (2013). Ley N.° 30096, Ley de Delitos Informáticos. Diario Oficial El Peruano.
- Consejo de la Unión Europea. (2023). Directiva (UE) 2023/2226 del Consejo, de 17 de octubre de 2023, por la que se modifica la Directiva 2011/16/UE relativa a la cooperación administrativa en el ámbito de la fiscalidad. Diario Oficial de la Unión Europea.
- Crumbley, D. L., Heitger, L. E., & Smith, G. S. (2017). Forensic and investigative accounting (8th ed.). CCH, a Wolters Kluwer business.
- Dirección Nacional de Ingresos Tributarios. (2026). Resolución General DNIT Nº 47/2026. https://www.dnit.gov.py/
- Eashrak, N., Hossain, M. I., Auyon, M. O. S. y Adnan, A. A. (2026). Forensic analysis of cryptocurrency transactions: Leveraging blockchain for fraud detection and regulatory compliance. En J. Choudrie, E. Tuba, T. Perumal y A. Joshi (Eds.), ICT for intelligent systems (pp. 487–503). Springer. https://doi.org/10.1007/978-981-95-1357-4_38
- Estado Plurinacional de Bolivia. Decreto Supremo N.º 5384 de 7 de mayo de 2025, sobre Empresas de Tecnología Financiera, activos virtuales, activos tokenizados, blockchain y PSAV.
- Ethereum Foundation. (2026). Ethereum documentation. https://ethereum.org/
- Etherscan. (2026). Etherscan developer documentation. https://docs.etherscan.io/
- European Commission. (s. f.). DAC8: Directive on Administrative Cooperation—Tax transparency for crypto-assets. Taxation and Customs Union. Recuperado el 7 de agosto de 2026.

- Financial Action Task Force. (2021). Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html
- Financial Action Task Force. (2023). Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. https://www.fatf-gafi.org/en/publications/Virtualassets/Guidance-rba-virtual-assets-2023.html
- Financial Action Task Force. (2023). Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Targeted-update-virtual-assets-vasps-2023.html
- Financial Action Task Force. (2023). The FATF Recommendations. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html
- Financial Action Task Force. (2025). Targeted update on implementation of the FATF standards on virtual assets/VASPs. FATF.
- Financial Action Task Force. (s. f.). FATF glossary. Recuperado el 7 de agosto de 2026.
- Financial Stability Board. (2023a). High-level recommendations for the regulation, supervision and oversight of crypto-asset activities and markets: Final report.
- Financial Stability Board. (2023b). High-level recommendations for the regulation, supervision and oversight of global stablecoin arrangements: Final report.
- Financial Stability Board. (2025a). FSB Plenary sets out 2026 work plan.
- Financial Stability Board. (2025b). Thematic review on FSB global regulatory framework for crypto-asset activities.
- Financial Stability Board. (2026). Promoting global financial stability: 2025 FSB annual report.
- Freeman, L. C. (1979). Centrality in social networks: Conceptual clarification. Social Networks, 1(3), 215–239. https://doi.org/10.1016/0378-8733(78)90021-7
- Fröwis, M., Gottschalk, T., Haslhofer, B., Rückert, C. y Pesch, P. (2020). Safeguarding the evidential value of forensic cryptocurrency investigations. Forensic Science International: Digital Investigation, 33, 200902. https://doi.org/10.1016/j.fsidi.2019.200902
- FSB. High-level Recommendations for the Regulation, Supervision and Oversight of Global Stablecoin Arrangements, 2023.

- Garratt, R., & van Oordt, M. R. C. (2023). The crypto multiplier (BIS Working Papers No. 1104). Bank for International Settlements.
- Grupo de Acción Financiera de Latinoamérica (GAFILAT). (2023). Buenas prácticas y documentos técnicos sobre enfoque basado en riesgos para activos virtuales. https://www.gafilat.org/
- Grupo de Acción Financiera de Latinoamérica (GAFILAT). (2023). Documentos técnicos y guías sobre transparencia y beneficiario final. https://www.gafilat.org/
- Hyperledger Foundation. (2026). Hyperledger Fabric documentation. https://hyperledger-fabric.readthedocs.io/
- IFRS Foundation. (2018). Conceptual Framework for Financial Reporting. https://www.ifrs.org/
- IFRS Foundation. (2024). IFRS 18 presentation and disclosure in financial statements. IFRS Foundation.
- IFRS Foundation. (2024). Issued IFRS Accounting Standards. https://www.ifrs.org/
- IFRS Foundation. (2026). IFRS Accounting Standards—Required 1 January 2026. IFRS Foundation.
- IFRS Interpretations Committee. (2019). Agenda Decision—Holdings of Cryptocurrencies. IFRS Foundation. https://www.ifrs.org/
- IFRS Interpretations Committee. (2019). Holdings of cryptocurrencies—Agenda Paper 12. IFRIC Update, June 2019. IFRS Foundation.
- IMF–FSB. Synthesis Paper: Policies for Crypto-assets, 2023.
- Institute of Internal Auditors. (2024). Global internal audit standards. IIA. https://www.theiia.org/en/standards/2024-standards/global-internal-audit-standards/
- International Auditing and Assurance Standards Board. (2019). ISA 315 (Revised 2019): Identifying and assessing the risks of material misstatement. International Federation of Accountants.
- International Auditing and Assurance Standards Board. (2022). Manual de pronunciamientos Interamericanaes de gestión de la calidad, auditoría, revisión, otros encargos de aseguramiento y servicios relacionados. https://www.ifac.org/publications/international-quality-management-auditing-review-other-assurance-and-related-services-pronouncements
- International Auditing and Assurance Standards Board. (2023). Handbook of International Quality Management, Auditing, Review, Other Assurance, and Related Services Pronouncements. International Federation of Accountants. https://www.ifac.org/

- International Auditing and Assurance Standards Board. (2024). 2023–2024 handbook of international quality management, auditing, review, other assurance, and related services pronouncements. International Federation of Accountants.
- International Auditing and Assurance Standards Board. (2025). ISA 240 (Revised): The auditor's responsibilities relating to fraud in an audit of financial statements. International Federation of Accountants.
- International Auditing and Assurance Standards Board. (2026). ISA 500 series. International Federation of Accountants.
- International Monetary Fund & Financial Stability Board. (2023). IMF-FSB Synthesis Paper: Policies for Crypto-Assets. https://www.imf.org/
- International Organization for Standardization. (2012). ISO/IEC 27037:2012. Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. ISO. https://www.iso.org/standard/44381.html
- International Organization of Securities Commissions. (2023a). Policy recommendations for crypto and digital asset markets: Final report (FR11/23). IOSCO.
- International Organization of Securities Commissions. (2023b). Final report with policy recommendations for decentralized finance (DeFi) (FR14/23). IOSCO.
- Internet Archive. (2026). Wayback Machine. https://web.archive.org/
- Mempool. (2026). Bitcoin explorer. https://mempool.space/
- Ministerio Público–Fiscalía de la Nación. (2006). Reglamento de la cadena de custodia de elementos materiales, evidencias y administración de bienes incautados (Resolución de la Fiscalía de la Nación N.° 729-2006-MP-FN).
- Moreira Mero, J. E., Lucas Pinargote, J. A., & Correa Cando, M. A. (2024). La auditoría forense en la era digital: Retos y estrategias de adaptación en Latinoamérica. https://doi.org/10.23857/dc.v10i3.3985
- Moreno Mahecha, L. E. (2022). Auditoría forense. Ediciones de la U. https://edicionesdelau.com/producto/auditoría-forense/
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
- OECD. Tokenisation of assets and distributed ledger technologies in financial markets, 2025.
- Organisation for Economic Co-operation and Development. (2019). Model tax convention on income and on capital 2017: Full version. OECD Publishing. DOI: 10.1787/g2g972ee-en.

- Organisation for Economic Co-operation and Development. (2020). Taxing virtual currencies: An overview of tax treatments and emerging tax policy issues. OECD Publishing. DOI: 10.1787/e29bb804-en.
- Organisation for Economic Co-operation and Development. (2023). International Standards for Automatic Exchange of Information in Tax Matters. https://www.oecd.org/
- Organisation for Economic Co-operation and Development. (2023). International standards for automatic exchange of information in tax matters: Crypto-Asset Reporting Framework and 2023 update to the Common Reporting Standard. OECD Publishing. DOI: 10.1787/896d79d1-en.
- Organisation for Economic Co-operation and Development. (2024). Crypto-Asset Reporting Framework and amended Common Reporting Standard: OECD releases IT format for transmitting information and issues interpretative guidance. OECD.
- Organisation for Economic Co-operation and Development. (2025a). Crypto-Asset Reporting Framework: 2025 monitoring and implementation update. Global Forum on Transparency and Exchange of Information for Tax Purposes. OECD.
- Organisation for Economic Co-operation and Development. (2025b). Crypto-Asset Reporting Framework XML Schema (July 2025): User guide for tax administrations. OECD Publishing. DOI: 10.1787/6e60235b-en.
- Organisation for Economic Co-operation and Development. (s. f.). Global Forum on Transparency and Exchange of Information for Tax Purposes. Recuperado el 7 de agosto de 2026.
- Parlamento Europeo y Consejo de la Unión Europea. (2023). Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010, (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (MiCA). Official Journal of the European Union, L 150, 40–205. https://eur-lex.europa.eu/
- Perú, Poder Ejecutivo. (2012). Decreto Legislativo N.° 1106, Decreto Legislativo de lucha eficaz contra el lavado de activos y otros delitos relacionados a la minería ilegal y crimen organizado. Diario Oficial El Peruano.
- Perú, Poder Ejecutivo. (2023). Decreto Supremo N.° 006-2023-JUS, que incorpora a los proveedores de servicios de activos virtuales como sujetos obligados a informar a la UIF-Perú. Diario Oficial El Peruano.
- Polygon Technology. (2026). Polygon technology. https://polygon.technology/

- Publicaciones institucionales sobre blockchain, DLT y banca Interamericana
- R3. (2026). Corda documentation. https://docs.r3.com/
- Scientific Working Group on Digital Evidence. (2024). Best Practices for Digital Evidence Collection and Preservation. https://www.swgde.org/documents
- Secretaría de Prevención de Lavado de Dinero o Bienes. (2020). Guía para Proveedores de Servicios de Activos Virtuales (PSAV). https://www.seprelad.gov.py/
- Secretaría de Prevención de Lavado de Dinero o Bienes. (2020). Resolución SEPRELAD Nº 08/2020 POR LA CUAL SE ESTABLECEN COMO SUJETOS OBLIGADOS DE LA LEY N° 1.015/97 Y SU MODIFICATORIA LA LEY Nº 3.783/09 Y LA LEY N° 6.497/19, A LAS PERSONAS FISICAS Y JURIDICAS QUE DESARROLLAN ACTIVIDADES ASOCIADAS CON ACTIVOS VIRTUALES. https://www.seprelad.gov.py/
- Secretaría de Prevención de Lavado de Dinero o Bienes. (2020). Resolución SEPRELAD Nº 09/2020 POR LA CUAL SE INSTA A LOS SUJETOS OBLIGADOS DE LA LEY N° 1.015/97 Y SUS LEYES MODIFICATORIAS A ADOPTAR EN SUS PROCESOS DE DEBIDA DILIGENCIA, CRITERIOS RELACIONADOS CON LAS PERSONAS FISICAS Y JURIDICAS QUE DESARROLLAN ACTIVIDADES ASOCIADAS CON ACTIVOS VIRTUALES. https://www.seprelad.gov.py/
- Solana Foundation. (2026). Solana documentation. https://solana.com/docs
- Solscan. (2026). Solana blockchain explorer. https://solscan.io/
- Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones. (2024). Resolución SBS N.° 02648-2024, Norma para la prevención del lavado de activos y del financiamiento del terrorismo aplicable a los proveedores de servicios de activos virtuales bajo supervisión de la UIF-Perú. SBS.
- The Institute of Internal Auditors. (2017). International Professional Practices Framework. The IIA. [Nota: desde 2025 rigen las Global Internal Audit Standards del IIA; el IPPF de 2017 debe leerse como antecedente histórico, no como marco vigente].
- Tribunal de Justicia de la Unión Europea. (2015, 22 de octubre). Skatteverket contra David Hedqvist (Asunto C-264/14, ECLI:EU:C:2015:718).
- Vouga Abogados. (2022). Aspectos regulatorios de los activos virtuales y el ecosistema Fintech en Paraguay. Asunción, Paraguay.

- Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). Blockchain technology overview (NISTIR 8202). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8202
- Ethereum.org. (s. f.). Transacciones. Recuperado el 22 de septiembre de 2026, de https://ethereum.org/es/developers/docs/transactions/
- Grupo de Acción Financiera Interamericana. (2020). Indicadores de alerta de blanqueo de capitales y financiamiento del terrorismo asociados a los activos virtuales. GAFI/OCDE. https://www.fatf-gafi.org/publications/fatfrecommendations/documents/Virtual-Assets-Red-Flag-Indicators.html

ISBN: 978-9945-9482-2-6